KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / tietoliikennetekniikka

Tero Kormu

SIMUNET-TESTIALUSTAN PERUSTAMINEN JA TESTITAPAUSTUTKIMUS

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma

KORMU, TERO	SimuNet-testialustan perustaminen ja testitapaustutkimus
Opinnäytetyö	52 sivua
Työn ohjaaja	yliopettaja Martti Kettunen
Toimeksiantaja	Kymenlaakson ammattikorkeakoulu / SimuNet-hanke
Tammikuu 2010	
Avainsanat	eompls, vpls, mpls, l2vpn-yhteys, virtuaaliverkot

Opinnäytetyö on tehty SimuNet-hankkeelle. SimuNet on osittain EAKR-rahoitteinen hanke, jonka osapuolia ovat Kymenlaakson ammattikorkeakoulun lisäksi alueen verkko-operaattorit.

Työn tarkoituksena oli rakentaa ja konfiguroida lähtökohta SimuNet-hankkeen perustana toimivalle SimuNet-verkolle Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorion palvelinhuoneeseen. Tavoitteena oli rakentaa todellisen Internet-palveluntarjoajan tuotantoverkon kaltainen T&K-verkko, joka edustaa uusinta tietoverkkotekniikkaa. Lisäksi tehtiin testitapaustutkimus, jossa tutkittiin SimuNet-verkon ja sen verkkolaitteiden soveltuvuutta MPLS-tekniikkaan perustuvien L2VPN-tekniikkaa käyttävien EoMPLS- ja VPLS-ratkaisumallien alustaksi.

Opinnäytetyön varsinaisen fyysisen rakennusvaiheen jälkeen konfiguroitiin toimiva IP/MPLS-verkko, jota käytettiin pohjana EoMPLS- ja VPLS-ratkaisujen toteuttamisessa. Verkkojen testausvaiheessa käytettiin apuna kuviteltuja yrityksen maantieteellisesti eri paikoissa sijaitsevia toimipaikkoja, joiden välille luotiin toimiva L2VPN-yhteys käyttäen EoMPLS- ja VPLS-tekniikkaa. EoMPLS-verkosta esitellään ja toteutetaan kaksi erilaista ratkaisumallia, joista ensimmäinen perustuu yksinkertaiseen porttitilaan ja toinen 802.1Q-tekniikkaa käyttävään ratkaisuun. VPLS-verkosta esitellään niin ikään kaksi erilaista ratkaisumallia, joista ensimmäinen perustuu access-kytkentään ja toinen 802.1Q-tekniikkaan perustuvaan ratkaisumalliin.

Työn tuloksena syntyi toimiva SimuNet-verkko ja toimivat EoMPLS- ja VPLS-ratkaisut, joita on tulevaisuudessa mahdollista käyttää pohjana SimuNet-hankkeessa ja SimuNet-verkkoa koskevissa T&K-töissä.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Electronics

KORMU, TERO	Establishment of SimuNet network and test study
Bachelor's Thesis	52 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Kymenlaakson ammattikorkeakoulu Oy / SimuNet Project
January 2010	
Keywords	eompls, vpls, mpls, virtual private network

The purpose of this thesis work was to set up a base network for the SimuNet project and perform a test study. In the test study the MPLS-based network and the suitability of its components for an L2VPN solution were investigated. The work was commissioned by the SimuNet project, which is partly funded by the European Regional Development Fund and has been commenced by Kymenlaakso University of Applied Sciences in association with the local Internet service providers.

The aim was to set up an R&D network that is similar to the production network of a real Internet service provider. The network would represent the newest technology.

First, the physical network was built in the server room of the telecommunications laboratory of Kymenlaakso University of Applied Sciences. After that, a working MPLS network was configured. The L2VPN solution was configured on top of the MPLS network using EoMPLS first and then VPLS. EoMPLS was configured in the port mode and the 802.1Q mode, while VPLS was configured in the access mode and 802.1Q modes. The testing phase was carried out by conducting a series of tests between two virtualized and geographically separate office departments.

The result of this study was a working SimuNet network with working EoMPLS and VPLS solutions. In the future they can be used in the SimuNet project or as a basis for further R&D studies.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

LYHENNELUETTELO

1 JOHDANTO 9

2 MPLS-TEKNIIKKA 10

2.1 MPLS-tekniikan toimintaperiaate 10

2.1.1 MPLS-kehys 11

2.1.2 MPLS-verkko 12

2.1.3 MPLS-kehyksien kytkeminen 13

2.1.4 LDP-yhteyskäytäntö 13

2.1.5 CEF-tekniikka 15

2.2 Reititysprotokollat 15

2.2.1 BGP-reititysprotokolla 17

2.2.2 OSPF-reititysprotokolla 17

2.3 L2VPN-tekniikka 20

2.3.1 EoMPLS-tekniikka 21

2.3.2 VPLS-tekniikka 22

3 LAITTEET 24

3.1 Cisco Catalyst 3560 -kytkin 24

3.2 Cisco 2821 -reititin 25

3.3 Cisco 7604 -reititin 26

3.4 Cisco SIP400 -lisämoduuli 28

3.5 Cisco ASA 5510 -palomuuri 28

3.6 SFP-moduuli 28

4 ASENNUKSET 30

4.1 Laitekaapin asennus 30

4.2 Laitteiden asennus laitekaappiin 30

4.3 SIP400-lisämoduulin asennus 7604-reitittimeen 30

4.4 SFP-moduulien asennus 31
4.5 Kaapelinvedot 32
4.6 Laitteiden IOS-päivitykset 32
4.6.1 2821-reitittimen IOS-päivitys 32
4.6.2 7604-reitittimen IOS-päivitys 33
5 SIMUNET-ALUSTAN TESTAUS EOMPLS-RATKAISULLA 34
5.1 Topologia 34
5.2 EoMPLS-verkon toteutus porttitilassa 35
5.3 EoMPLS-verkon toteutus VLAN-tilassa 36
5.4 EoMPLS-verkon toiminnan testaus 36
6 SIMUNET-ALUSTAN TESTAUS VPLS-RATKAISULLA 40
6.1 Topologia 40
6.2 Access-kytkentä 41
6.3 802.1Q trunk -kytkentä 41
6.4 VFI-instanssin konfigurointi 43
6.5 VPLS-verkon testaus 44
7 YHTEENVETO 48
LÄHTEET 50

LYHENNELUETTELO

ATM	Asynchronous Transfer Mode; pakettikytkentäinen tiedonsiirtoprotokolla
AToM	Any Transport over MPLS; Ciscon tekniikka Layer 2 -kehysten siirtämiseen IP/MPLS-verkon yli
ARP	Address Resolution Protocol; selvittää IP-osoitetta vastaavan MAC-osoitteen
BDR	Backup Designated Router; OSPF-protokollan varareititin
CEF	Cisco Express Forwarding; Layer 3 -kytkemisteknologia tietoverkoissa
DR	Designated Router; OSPF-protokollan pääreititin
E-LAN	Ethernet LAN; Layer 2 -vpn-tekniikka
E-LINE	Ethernet LAN; Layer 2 -vpn-tekniikka
EAKR	Euroopan aluekehitysrahasto
EGP	Exterior Gatewar Protocol; reititysprotokollaryhmä
EIGRP	Enhanced Interior Gateway Routing Protocol; reititysprotokolla
EoMPLS	Ethernet over MPLS; Layer 2 -vpn-tekniikka
FEC	Forwarding Equivalence Class; MPLS-tekniikassa IP-osoitteiden ryhmä
FIB	Forwarding Information Base; MPLS-tekniikassa reititystaulu

IETF	Internet Engineering Task Force; Internet-protokollien standardoinnista vastaava organisaatio
IGP	Interior Gateway Protocol; reititysprotokollaryhmä
IOS	Internetwork Operating System; Cisco-laitteiden komentorivipohjainen käyttöjärjestelmä
IPv4	Internet Protocol version 4; Internet-protokollan versio 4
IPv6	Internet Protocol version 6; Internet-protokollan versio 6
IS-IS	Intermediate System-to-Intermediate System; reititysprotokolla
L2VPN	Layer 2 VPN; toisen siirtokerrostason VPN-yhteys
L3VPN	Layer 3 VPN; kolmannen siirtokerrostason VPN-yhteys
LAN	Local Area Network; lähiverkko
LDP	Label Distribution Protocol; yhteyskäytäntö MPLS-verkossa
LFIB	Label Forwarding Information Base; MPLS-reitittimen tietokanta reiteistä
LIB	Label Information Base; MPLS-reitittimen tietokanta MPLS-lipuista
LSR	Label Switch Router; MPLS-reititin
MAC	Media Access Control; Layer 2 -tason osoite
MEF	Metro Ethernet Forum; Carrier Ethernet -tekniikan kehittäjä

MPLS	Multiprotocol Label Switching; tiedonsiirtomenetelmä ilman IP-pakettien reititystä
OSI	Open Systems Interconnection Reference Model; tiedonsiirtomalli
OSPF	Open Shortest Path First; reititysprotokolla
QinQ	IEEE 802.1QinQ; standardi Ethernet-kehysformaatille
QoS	Quality of Service; palvelunlaatu
RIP	Routing Information Protocol; reititysprotokolla
SFP	Small form-factor pluggable transceiver; lähetin-vastaanotin tietoliikenteessä
TCP	Transmission Control Protocol; tietoliikenneprotokolla
UDP	User Datagram Protocol; yhteyskäytäntö
VLAN	Virtual Local Area Network; virtuaalilähiverkko
VPLS	Virtual Private LAN Service; Layer 2 -vpn-tekniikka
VPN	Virtual Private Network; näennäisesti yksityinen verkko

1 JOHDANTO

Työn tarkoituksena oli perustaa SimuNet-verkko Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorion palvelinhuoneeseen ja tämän jälkeen tehdä testitapaustutkimus, jossa selvitettiin SimuNet-verkon soveltuvuutta erilaisille MPLS-tekniikkaan perustuville ratkaisuille. Testitapaustutkimukseen sisältyi perehtyminen L2VPN-maailmaan, joka pitää sisällään mm. EoMPLS - ja VPLS-tekniikan. Perehtymisen jälkeen oli tarkoitus rakentaa toimiva IP/MPLS-verkko ja sen päälle toimiva L2VPN-tekniikkaa käyttävä VPN-ratkaisu. Laitteina käytettiin SimuNet-hankkeen laitteita. Niiden fyysinen asennus sekä konfigurointi kuului myös työhön.

SimuNet-hanke on EAKR (Euroopan aluekehitysrahasto) -hanke, jossa ovat mukana Kymen Puhelin Oy, Optimiratkaisut Oy, Haminan Energia Oy, Loviisan Puhelin Oy ja Cursor Oy. Myös Otsakorven säätiö on rahoittanut hanketta. Hankkeessa on tavoitteena rakentaa todellisen Internet-palveluntarjoajan tuotantoverkon kaltainen T&K-verkko, joka edustaa uusinta tietoverkkotekniikkaa. SimuNet-verkkoon liitetään myöhemmin kahdennetut palvelin- ja palomuuriratkaisut sekä simuloituja asiakkaiden yritysverkkoja mutta niiden käsittely ei sisälly tähän opinnäytetyöhön.

SimuNet-verkon avulla on tarkoitus simuloida niitä Internet-palveluntarjoajan haasteita, joita uusien tekniikoiden sisällyttäminen tuotantoverkkoon aiheuttaa. Tavoitteena on rakentaa SimuNet-verkosta etäkäytettävä kokonaisuus. SimuNet-verkkoa on tarkoitus hyödyntää perusopetuksessa, projektiopinnoissa, erikoistumisopinnoissa ja yrityksille tarjottavissa kursseissa. Simunet-verkon avulla on tarkoitus toteuttaa työelämälähtöisiä projekteja ja opinnäytetöitä, jotka liittyvät verkkoratkaisujen käytettävyyteen, luotettavuuteen, tietoturvaan tai palvelunlaatuun. (1, 23-25)

Työssä keskitytään tarkastelemaan L2VPN-pohjaisia ratkaisuja ja ratkaisumalleja, joten L3VPN-ratkaisut on rajattu työn ulkopuolelle. Kaikki tässä työssä käytettävät palveluntarjoajan kuljetusverkkoratkaisut pohjautuvat IP/MPLS-tekniikkaan. Työssä ei käsitellä muita mahdollisia kuljetusverkkoratkaisuja, kuten esimerkiksi QinQ-tekniikkaa, jolla on mahdollista toteuttaa samankaltainen ympäristö. Työssä käytetty terminologia on myös hieman Cisco-painoitteista, koska kaikki tässä työssä käytettävät verkkolaitteet olivat Cisco Systemsin valmistamia.

2 MPLS-TEKNIIKKA

1990-luvun alkupuolella ATM (Asynchronous Transfer Mode) ja IP (Internet Protocol) -tekniikat olivat laajasti käytössä. Näiden tekniikoiden yhteensopivuutta haluttiin kuitenkin parantaa. Laitteiden valmistajat, kuten IBM, Cisco Systems ja Toshiba, toivat aluksi markkinoille omia epävirallisia ratkaisujaan. Kuitenkin vuonna 1997 IETF (Internet Engineering Task Force) perusti työryhmän, jonka tarkoitus oli tekniikan standardointi. Näin syntyi tekniikka, josta käytetään nykyisin nimeä MPLS (Multiprotocol Label Switching). (2, 263–272)

MPLS-tekniikan kehitykseen osallistuu IETF:n ohella monia tahoja, kuten esimerkiksi Broadband Forum. Sen jäseniin kuuluu niin tietoliikennealan asiantuntijoita, laitteiden valmistajien edustajia kuin myös Internet-palveluntarjoajien edustajia. (3)

Seuraavassa MPLS-tekniikan periaatteita. Käytetty tekniikka ja terminologia vaihtelevat hieman valmistajakohtaisesti. Tässä työssä Simunet-verkkoon valittiin Cisco Systemsin laitteet. Teoriaa ja terminologiaa on käsitelty näiden laitteiden näkökulmasta.

2.1 MPLS-tekniikan toimintaperiaate

MPLS-tekniikka on samankaltainen kuin ATM-tekniikka, mutta se toimii tavalla, joka sopii paremmin IP-protokollan tarpeisiin. MPLS-tekniikka käyttää lippuja (label), joiden avulla reitittimet kytkevät paketteja. Lippu edustaa sitä FEC (Forwarding Equivalence Class) -luokkaa, johon paketti kuuluu. Nämä liput kiinnitetään IP-paketteihin, minkä jälkeen reititin kytkee ne lipun perusteella tavallisen IP-reitityksen sijasta. (4, 5)

IP-reitityksessä reititin tutkii IP-paketin otsikkokentästä IP-osoitteen, johon paketti on tarkoitus reitittää. Tämän jälkeen reititin tarkistaa reititystaulustaan, mihin paketti kuuluisi reitittää. Reitittämistä seuraavalle reitittimelle kutsutaan hypyksi. MPLS-tekniikassa seuraavan hypyn valinta on kaksivaiheinen operaatio. Ensin paketit luokitellaan määränpäänsä mukaan FEC-luokkiin, jotka pitävät sisällään monia kohdeosoitteita. Kaikki paketit, jotka kuuluvat samaan FEC-luokkaan, saavat osakseen saman kohtelun. Tämän jälkeen jokaiselle FEC-luokalle valitaan seuraava hyppy. (5, 3–5)

Frame Relay- ja ATM-tekniikka ovat käyttäneet vastaavaa tekniikkaa jo kauan kuljettaakseen kehyksiä ja soluja verkossa, joten tekniikka ei ole uusi. Frame Relay -tekniikassa kehyksen koko vaihtelee, kun taas ATM-tekniikassa solu on aina tietyn kokoinen. Solu koostuu viiden tavun kokoisesta otsikosta ja 48 tavun kokoisesta hyötykuormasta. ATM-solun otsikko ja Frame Relayn kehys viittaavat virtuaaliseen alueeseen, jossa solu tai kehys sijaitsee. Yhtäläisyys Frame Relayn ja ATM:n välillä on se, että tietoverkossa jokaisen hypyn välillä lipun arvoa muutetaan. Tämä eroaa hieman IP-pakettien reitityksestä. Kun reititin reitittää IP-paketin, se ei vaihda paketin kohdeosoitetta. MPLS-tekniikasta on tehnyt suositun se, että MPLS-lippuja käytetään reitittämiseen kohdeosoitteen sijasta. (5, 287; 6, 198; 7, 155)

MPLS-tekniikka mahdollistaa tehokkaamman toiminnan perinteiseen IP-reititykseen verrattuna, koska paketteja ei käsitellä verkkokerroksella. Kytkentä tapahtuu FEC-taulun avulla ja se tehdään vain kerran. Muut verkossa olevat reitittimet eivät käytä resurssejaan paketin otsikon tutkimiseen, vaan reititys tapahtuu MPLS-lipun avulla. (5, 8–9)

2.1.1 MPLS-kehys

MPLS-tekniikassa käytetään kehystä, joka lisätään OSI-mallin (Open Systems Interconnection Reference Model) siirtokerroksen ja verkkokerroksen väliin.

Kuva 1. MPLS-kehys

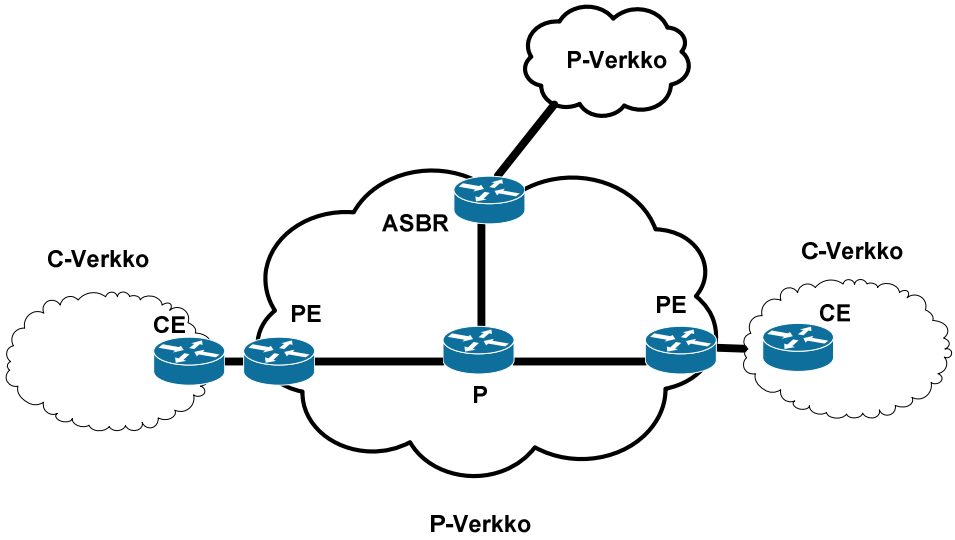
Kuvassa 1 on esitetty MPLS-kehyksen rakenne. Kehys on 32 bitin mittainen ja sen rakenne on aina tietynlainen. Ensimmäiset 20 bittiä pitävät sisällään varsinaisen lipun tunnisteen. Kolmen bitin mittainen EXP (Experimental) -kenttä on tarkoitettu MPLS-palvelujen käyttöön. Yleensä sitä käytetään QoS-palveluiden (Quality of Service) kanssa. MPLS-kehyksen perään lisätään varsinainen IP-paketti, joka säilyy koskemattomana lipun määräämään paikkaan asti. (8, 2–3)

S-bitti asetetaan ykköseksi silloin, kun kyseessä on viimeinen kehys ennen varsinaista IP-pakettia. Muussa tilanteessa S-bitti on aina nolla. Lippuja voidaan pinota päällek-

käin S-bitin avulla. TTL (Time to Live) -kentällä on sama merkitys kuin IP-paketin TTL-kentällä. Sen avulla määritetään kehyksen elinaika verkossa. Jokaisen hypyn jälkeen TTL-kentän sen hetkisestä arvosta vähennetään yksi. Kun kentän arvo on nolla, reititin poistaa kehyksen verkosta. Näin ehkäistään silmukat verkoissa. (8, 2–3)

2.1.2 MPLS-verkko

MPLS-verkko muodostuu laitteista, joista jokaisella on oma tehtävänsä MPLS-verkon toiminnassa.



Kuva 2. MPLS-verkko

Kuvasta 2 nähdään MPLS-verkon perusrakenne. MPLS-verkko koostuu seuraavista laitteista:

P-verkko: Palveluntarjoajan MPLS/IP-runkoverkko, joka luo pohjan MPLS-tekniikalle ja VPN-yhteyksille.

P-reititin: Palveluntarjoajan reititin P-verkon sisällä, sillä ei ole minkäänlaisia reunareitittimen toimintoja. Reititin toimii siis vain välittäjänä.

PE-reititin**:** Palveluntarjoajan reunareititin, jonka tehtävän on tarjota asiakkaalle esimerkiksi MPLS/VPN-yhteys kahden toimipisteen välillä.

ASBR-reititin**:** Reititin, jonka tehtävänä on toimia palveluntarjoajan yhden autonomisen alueen reunareitittimenä.

C-verkko**:** Asiakkaan oma verkko, joka on asiakkaan itsensä ylläpitämä.

CE-reititin**:** Reititin, joka tarjoaa yhdyskäytävän C-verkon ja P-verkon välille. CE-reititin voi olla asiakkaan tai palveluntarjoajan ylläpitämä. (9, 5)

2.1.3 MPLS-kehyksien kytkeminen

Reitintä, joka kytkee MPLS-kehyksiä, kutsutaan LSR:ksi (Label switch router). LSR ymmärtää MPLS-kehyksiä ja vastaanottaa sekä lähettää lippupaketteja siirtokerroksella. MPLS-verkon reunalla oleva reititin lisää lipun paketin eteen, ennen kuin se kytketään MPLS-verkkoon. Kun paketti poistuu MPLS-verkosta, reunalla oleva reititin poistaa paketin edestä lipun ja lähettää sen tavalliseen IP-verkkoon. (4, 29; 8, 3–5)

Joissakin tilanteissa saatetaan joutua lisäämään monta kehystä päällekkäin, jotta paketti voidaan kytkeä MPLS-verkon yli. Kun reititin saa kehyksen, se katsoo aina päällimmäisenä olevan lipun arvoa. Tämän jälkeen reititin tietää, mihin ja miten paketti kuuluu kytkeä. Lipun merkitys ei kuitenkaan ole koskaan sama kaikilla reitittimillä, vaan lipun arvo on merkityksellinen vain kahden reitittimen välillä. Lipun arvo määräytyy FEC-luokan mukaan. Reititin saattaa joutua tekemään paketille toimenpiteitä ennen sen kytkemistä eteenpäin. Toimenpiteitä on kolme erilaista:

1. Reititin vaihtaa päällimmäisen lipun arvon toiseksi (SWAP).
2. Reititin poistaa arvon kehyksestä (POP).
3. Reititin vaihtaa päällimmäisen lipun arvon ja sen jälkeen lisää vielä yhden tai enemmän arvoja lippupinoon (PUSH).

Näiden toimintojen lisäksi reititin oppii lipussa olevasta arvosta siirtokerroksen kapseloinnin sekä joitakin muita toimenpiteitä, joilla lipun voi kytkeä eteenpäin. (8, 3–5)

2.1.4 LDP-yhteyskäytäntö

Kahden LSR-reitittimen täytyy kommunikoida jotenkin keskenään, jotta ne voivat sopia MPLS-lippujen arvojen merkityksistä. Tämä tehdään käyttämällä LDP (Label Distribution Protocol) -yhteyskäytäntöä. LDP-protokolla ei ole kuitenkaan ainut tähän tarkoitukseen sopiva sidostenvaihtoprotokolla. (10, 4)

LDP-protokollan päätarkoitus on mainostaa sidoksia naapurireitittimelle. Kun kaikilla LSR-reitittimillä on liput tietylle FEC-luokalle, paketit voidaan kytkeä verkon yli lippujen avulla. Esimerkiksi SimuNet-verkossa käytetyissä Cisco Systemsin laitteissa LSR-reititin tietää lipulle tehtävän toiminnon katsomalla LFIB-taulua (Label Forwarding Information Base). LDP-protokolla syöttää vastaanottamansa sidokset LIB:een (Label Information Base), joka taas syöttää ne eteenpäin LFIB-tauluun. LDP-istunto täytyy muodostaa reitittimien välille, jotta reitittimet voivat vaihtaa viestejä keskenään. Lippusidos on lippu, jolla on oma FEC-luokkansa. (4, 68–77; 11)

LDP-yhteyskäytännöllä on neljä päätarkoitusta:

1. Toisten LDP-protokollaa käyttävien LSR-reitittimien havainnointi
2. Istunnon aloitus ja ylläpito
3. Sidoksien mainostus
4. Tiedotusviestit tapahtuneista virheistä

Kaksi vierekkäistä LDP-protokollaa käyttävää LSR-reititintä löytävät toisensa Hello-viestien avulla. Tämän jälkeen ne avaavat istunnon TCP-yhteyden avulla. Tämän TCP-yhteyden yli LDP-protokolla mainostaa sidoksiaan kahden reitittimen välillä. Näitä sidosviestejä käytetään sidoksien mainostamiseen,vaihtamiseen tai poistamiseen. LDP-protokolla pystyy ilmoittamaan LDP-naapurille virheviesteistä lähettämällä tiedotusviestejä. (10, 30–31)

LDP-protokollan Hello-viestit lähetetään kaikille yhteysväleille, joissa LDP-protokolla on sallittu. Yleensä tämä tarkoittaa kaikkia rajapintoja, joissa **mpls ip** -käsky on käytössä. LDP-protokollan Hello-viestit käyttävät UDP-protokollaa ja porttia 646. Hello-viestit pitävät sisällään pitoajan. Jos vastapuoli ei ole vastannut pitoajan kuluessa, olettaa reititin yhteyden olevan poikki. LDP-istuntoa ylläpitää LDP-pakettien vastaanottaja. Istuntoa voidaan myös ylläpitää jaksollisilla Keepalive-viesteillä. Joka kerta, kun vastaanottaja saa LDP-paketin tai Keepalive-viestin, Keepalive-aika nollautuu. (10, 50–54, 68–77)

2.1.5 CEF-tekniikka

CEF (Cisco Express Forwarding) -tekniikka on suunniteltu helpottamaan liikennevirtojen käsittelyä Simunet-verkon käyttämissä Cisco Systemsin laitteissa. Vanhemmat tekniikat joutuivat etsimään kohdetta reititystaulusta, ja tämä hidasti laitteen toimintaa paljon etenkin suurissa verkoissa, joissa reitittimillä on suuri määrä potentiaalisia kohdeosoitteita. Sen lisäksi jokaiselle paketille täytyi tehdä uusi toisen kerroksen otsikko. (4, 151–153; 12)

CEF käyttää välimuistia viimeisimpien käytettyjen kohteiden tallentamiseen. Toisin sanoen taulua ei tehdä vasta sitten, kun sitä tarvitaan, vaan se tehdään etukäteen. CEF käyttää FIB (Forwarding Information Base) -taulua tehdäkseen IP-kohdetta koskevia kytkemispäätöksiä. FIB-taulu on samantyylinen IP-reititystaulun kanssa. Se ylläpitää ns. peilikuvaa IP-reititystaulun reititystiedoista. Kun muutoksia tapahtuu verkossa, IP-reititystaulu päivitetään ja päivitykset heijastuvat myös FIB-tauluun. (4, 151–153; 12)

FIB-taulu ei ylläpidä tietoja lähtevistä rajapinnoista ja niitä vastaavista toisen kerroksen otsikoista, vaan tieto säilytetään erillisessä taulussa, jota kutsutaan naapuruustauluksi (Adjacency Table). Tämä taulu tarjoaa kopion ARP (Address Resolution Protocol) -välimuistista ja pitää sisällään toisen kerroksen otsikon. Laitteet voivat löytää toisensa dynaamisesti tai erillisten konfigurointien avulla. Ethernet-verkon tapauksessa on tärkeää, että reitittimet käyttävät dynaamista mekanismia toistensa löytämiseksi. Tämä mekanismi on ARP, joka kartoittaa toisen kerroksen osoitteet IP-osoitteiksi. (4, 151–153; 12)

Kun paketti saapuu reitittimelle, reititin irrottaa siitä Layer 2 -tiedon. Tämän jälkeen reititin etsii kohdeosoitetta FIB-taulusta ja tekee päätöksen edelleenlähettämisestä. Päätöksen kohde osoittaa yhteen naapuruuteen naapuruustaulussa, jonka avulla reititin asettaa paketille uuden Layer 2 -otsikon, ennen kuin paketti lähetetään eteenpäin. (4, 151–153; 12)

2.2 Reititysprotokollat

Saadessaan IP-paketin reititin tarvitsee reititystietoja, jotta se pystyy ohjaamaan paketit kohdeosoitteen perusteella sellaisiin verkkoihin, joihin reitittimellä ei ole suoraa yhteyttä. Verkon ollessa pieni voidaan staattisia reittejä konfiguroida reitittimelle kä-

sin. Staattiset reitit eivät kuitenkaan ota huomioon verkon muutoksia, minkä vuoksi paketit eivät välttämättä löydä perille. Ongelma kasvaa sitä mukaa, mitä suuremmaksi verkot kasvavat. Ratkaisuksi on kehitetty reititysprotokollat, jotka pitävät dynaamisesti kirjaa verkon rakenteesta ja sen muutoksista. (13, 110)

Reititysprotokollaa yhden autonomisen alueen sisällä kutsutaan IGP:ksi (Interior Gateway Protocol). IGP pitää sisällään monia erilaisia reititysprotokollia, joista on mahdollista valita tilanteeseen sopivin vaihtoehto. IGP:n tavoite on vastata nopeasti topologiamuutoksiin autonomisen alueen sisällä sekä tarjota nopea konvergenssi silmukkavapaaseen reititykseen. Käytettävän IGP:n on myös estettävä turhat reititystietojen muutokset, jotka aiheutuvat viallisista yhteysväleistä. (13, 28)

IGP:t voidaan jakaa kahteen ryhmään:

Etäisyysvektoriprotokollat

Etäisyysvektoriprotokollat käyttävät tietoja, jotka perustuvat yksinkertaisimmillaan pelkästään etäisyyteen. Reitittimen reititystaulussa on aluksi tieto suoraan reitittimessä kiinni olevista verkoista. Näihin verkkoihin etäisyys on nolla. Reititin lähettää tietyin väliajoin suoraan kytketyille reitittimille kopion omasta reititystaulustaan. Vastaanottaja etsii saaduista tiedoista sellaisia yhteyksiä, joita sen omasta reititystaulusta ei löydy. Etäisyysvektoriprotokollat laskevat etäisyyden kohteeseen hyppyjen määrällä eli kuinka monen reitittimen kautta paketin täytyy kulkea. Etäisyysvektoriprotokollia ovat esimerkiksi RIP (Routing Information Protocol) ja EIGRP (Enhanced Interior Gateway Routing Protocol). (14)

Linkin tila -protokollat

Linkin tila -protokolla toimii siten, että jokainen verkon reititin muodostaa eräänlaisen kartan yhteyksistään verkossa. Kukin reititin laskee loogisimman hypyn jokaiseen kohteeseen verkossa. Näistä hypyistä muodostuu reitittimen reititystaulu. Linkin tila -protokollassa reitittimet jakavat keskenään vain suoraan kytkettyjen reitittimien yhteystiedot koko reititystaulun sijasta. Linkin tila -protokollia ovat esimerkiksi OSPF (Open Shortest Path First) ja IS-IS (Intermediate System to Intermediate System). (14)

2.2.1 BGP-reititysprotokolla

Löytääkseen tietoverkoissa perille kohdeosoitteeseensa täytyy IP-paketin yleensä kulkea monen eri autonomisen alueen läpi. Jotta tämä on mahdollista, täytyy autonomisten alueiden kommunikoida jollakin tavalla keskenään. Autonomisten alueiden reunareitittimet vaihtavat reititystietoja keskenään käyttämällä reititysprotokollaa, joka kuuluu EGP (Exterior Gateway Protocol) -ryhmään. EGP on myös reititysprotokolla EGP-ryhmässä, joten näitä kahta ei saa sekoittaa keskenään. (15, 108)

Nykyään BGP (Border Gateway Protocol) on kuitenkin syrjäyttänyt EGP:n. BGP-reititysprotokollasta on olemassa standardi RFC 4271, johon tässäkin työssä viitataan. Autonomisen alueen sisällä käytettävästä BGP-protokollasta käytetään nimeä iBGP (Interior Border Gateway Protocol) ja autonomisten alueiden välillä puhutaan eBGP:sta (Exterior Border Gateway Protocol). BGP-naapurit määritellään manuaalisesti konfiguroimalla TCP-istunto porttiin 179. BGP-protokolla lähettää tietyin väliajoin 19-tavuisia viestejä pitääkseen yhteyden avoinna. (15, 7–8)

BGP:lla on käytössä kuusi erilaista tilaa, joilla se muodostaa yhteyden BGP-naapureiden välille. Tilat ovat **Idle**, **Connect**, **Active**, **OpenSent**, **OpenConfirm** ja **Established**. Idle-tilassa BGP kieltäytyy kaikista tulevista BGP-yhteysyrityksistä ja aloittaa TCP-yhteyden BGP-naapurin kanssa. Connect-tilassa reititin odottaa TCP-yhteyden valmistumista. Yhteyden onnistuessa tila siirtyy OpenSent-tilaksi ja reititin lähettää Open-viestin odottaen samaa vastapuolelta. Vasta vastauksen tultua reitittimien tila vaihtuu Established-tilaksi, jolloin reititin voi vaihtaa vastapuolen kanssa reititystietoja. Reitittimeen täytyy määritellä käsin viereisen BGP-protokollaa käyttävän reitittimen tiedot, jotta reititys onnistuu ja tieto siirtyy laitteiden välillä. (15, 52–74)

2.2.2 OSPF-reititysprotokolla

OSPF-protokolla on Linkin tila -algoritmia käyttävä reititysprotokolla, joka on tarkoitettu reititystietojen vaihtamiseen reitittimien kesken IP-verkoissa. OSPF-protokolla kuuluu IGP-ryhmään ja toimii yhden autonomisen alueen sisällä. OSPF-protokollasta on olemassa kaksi standardia: RFC 2328, joka on tarkoitettu IPv4-tekniikalle, ja RFC 5340, joka on tarkoitettu IPv6-tekniikalle. (16, 5)

Työssä on valittu käytettäväksi OSPF-protokolla muiden IGP-protokollien sijasta, joten se käsitellään muita protokollia tarkemmin.

RFC 2328 -standardin mukaan OPSF:n toiminta perustuu yhteystietoihin, joita reitittimet lähettävät toisilleen. Jokainen OSPF-reititin ylläpitää tietokantaa, jossa kuvataan kyseessä olevan autonomisen alueen topologiaa. Tämän tietokannan pohjalta rakennetaan reititystaulu käyttämällä lyhyimpiä reittejä. Reitit lasketaan tarvittaessa nopeasti uudelleen topologian muuttuessa ja muuttuneiden yhteyksien mainostamiseen käytetään hyvin vähän kaistanleveyttä. (16, 12–16)

Reititystaulun rakentamiseen liittyy tiettyjä käytäntöjä. Reittien valintaan vaikuttavat tietyt kertoimet jokaisella reititysrajapinnalla. Näitä ovat etäisyys reitittimeen, yhteysvälin kaistanleveys ja nopeus, saatavuus ja luotettavuus. Yhteysvälit, jotka saavat saman arvon, voivat jakaa tiedonsiirrosta aiheutuvan kuorman keskenään. Reitittimet saman toimialueen alla muodostavat yhteyksiä keskenään saatuaan toisiltaan OSPF Hello -paketteja. Ethernet-verkossa reitittimet valitsevat keskenään joukostaan DR (Designated Router) -reitittimen ja BDR (Backup Designated Router) -reitittimen, jotka toimivat keskittiminä ja vähentävät liikennettä muiden reitittimien kesken. (16, 8–10; 15–17; 53–57)

DR-reitittimen valintaan vaikuttaa OSPF-reitittimen prioriteettiarvo. Prioriteettiarvo voi olla mikä tahansa väliltä 0–254. Jos arvo on nolla, ei reititin voi koskaan olla DR- tai BDR-reititin. Jos nykyinen DR-reititin katoaa verkosta, BDR-reitittimestä tulee uusi DR-reititin ja reitittimet valitsevat keskuudestaan uuden BRD-reitittimen. Prioriteettiarvo siirtyy Hello-paketeissa. Jos kahdella tai useammalla on sama suurin prioriteettiarvo, se reititin, jonka RID (Router ID) -arvo on suurin, tulee valituksi. (16, 53–57)

Jos verkkoon ilmestyy valinnan jälkeen reititin, jonka prioriteettiarvo on suurempi, siitä ei tule uutta DR- tai BDR-reititintä, ennen kuin edellinen DR- tai BDR-reititin häviää verkosta. (16, 53–57)

DR-reititin vähentää verkon liikennettä olemalla eräänlainen keskitin verkossa. Se toimii reittipäivitystietojen lähteenä, ylläpitää kokonaista topologiataulua verkosta ja lähettää päivitykset muille reitittimille monilähetyksenä (multicast). Kaikki alueen reitittimet muodostavat yhteyden vain DR- ja BDR-reitittimiin. Reitittimet lähettävät päivitystietonsa DR- ja BDR-reitittimille monilähetyksenä osoitteeseen 224.0.0.6,

minkä jälkeen DR-lähettää kyseisen päivityksen kaikille samassa alueessa oleville reitittimille osoitteeseen 224.0.0.5. Monilähetystekniikka vähentää huomattavasti verkon liikennettä, koska yksi viesti kulkee samalla kaikille. Poin-to-Point-yhteysväleillä ei valita DR- tai BDR-reititintä, koska reitittimet ovat vierekkäin ja niiden välistä kaistanleveyttä ei ole enää mahdollista optimoida. (16, 53–57)

OSPF ei käytä ulkopuolista siirtoprotokollaa, vaan omaa tunnistettaan IP-protokollanumerolla 89. Näin ollen OSPF pitää itse huolta virheistä ja niiden korjaamisesta. OSPF reitittää IP-paketit niiden otsikosta löytyvän kohdeosoitteen mukaan, eikä niitä kapseloida millään tavalla. Verkko voidaan jakaa alueisiin (Area) ja näin hallinnoida reititystä. Yhden alueen sisäinen topologia ei näy alueen ulkopuolelle muille saman autonomisen alueen alueille, mikä vähentää tarvittavaa reititysliikennettä merkittävästi. (16, 185)

Alue nolla on aina koko OSPF-verkon ydin. Jokaisella alueella täytyy olla fyysinen tai virtuaalinen yhteys verkon ytimeen. Reunareititin ylläpitää tällaisia yhteyksiä ja tietokantaa jokaisesta alueesta, jonka kanssa se on yhteydessä. Alueet mainostavat tiivistettyjä osoitejoukkoja alueen ulkopuolelle ja ytimelle. (16, 26; 223)

Muut OSPF-alueet voidaan jakaa seuraaviin alueisiin:

Stub-alue

Stub-alue ei saa reittejä autonomisen alueen ulkopuolelta ja kaikki ulospäin lähtevä liikenne siirtyy oletusreitin avulla. Siten vähennetään reititystietokantojen kokoa alueen sisällä olevissa reitittimissä.

Not-so-stubby-alue

Not-so-stubby-alue hyväksyy alueen ulkopuoliset reitit, mutta ei mainosta niitä eteenpäin.

Totally stubby -alue

Totally stubby -alue on samankaltainen Stub-alueen kanssa ja siihen pätevät samat säännöt. Lisäksi alue ei salli tiivistettyjen osoitejoukkojen reittejä alueen ulkopuolelta. (16, 36–38; 17)

Jokaisella OSPF-reitittimellä on tunniste, joka on IP-osoitteen tapainen. Yleensä reitittimeen konfiguroidaan oma Loopback-osoitteensa, jota käytetään myös OSPF-tunnisteena. Jos tällaistä tunnistetta ei kuitenkaan ole konfiguroitu, muodostuu se korkeimmasta loogisesta reitittimen rajapintoihin konfiguroidusta IP-osoitteesta. (16, 46)

2.3 L2VPN-tekniikka

VPN (Virtual Private Network) -tekniikan avulla mahdollistetaan virtuaalinen verkko, joka toimii fyysisen verkon päällä muodostaen näin näennäisesti yksityisen verkon julkisen verkon ylitse. VPN-verkko voidaan salata joko fyysisesti tai erillisellä salauksella. (18, 4–5)

Tässä työssä käsitellään fyysisiä VPN-verkkoja, joista on olemassa L2VPN- ja L3VPN-ratkaisuja. Tämä työ pitää sisällään vain erilaisia L2VPN-ratkaisuja, eikä L3VPN-ratkaisuja tai tekniikkaa käsitellä ollenkaan.

Layer 2 -tason VPN-yhteydet on jaettu kahteen eri kategoriaan: E-Line (Ethernet Line) ja E-LAN (Ethernet Lan). Ne on kehittänyt MEF (Metro Ethernet Forum). MEF on yritysten yhdistymä, joka on perustettu kehittämään ja markkinoimaan Ethernet tiedonsiirtoverkoissa käytettäviä palveluja. MEF luo ehdotuksia Ethernet Carrier -verkkoon liittyvistä standardeista, joita laitevalmistajat ja palveluntarjoajat ottavat käyttöön. (19)

E-line-ratkaisussa käytetään virtuaalikanavaa ulkoverkon yli. Virtuaalikanavan päätepisteet ovat LAN-verkossa yhteydessä keskenään, mutta minkäänlaista Layer 2 -tason jäljittelyä ei tapahdu. PE-laitteet kuljettavat saamansa kehykset automaattisesti virtuaalikanavan toiselle puolelle. E-Line on siis yksinkertainen LAN-ratkaisu. (19)

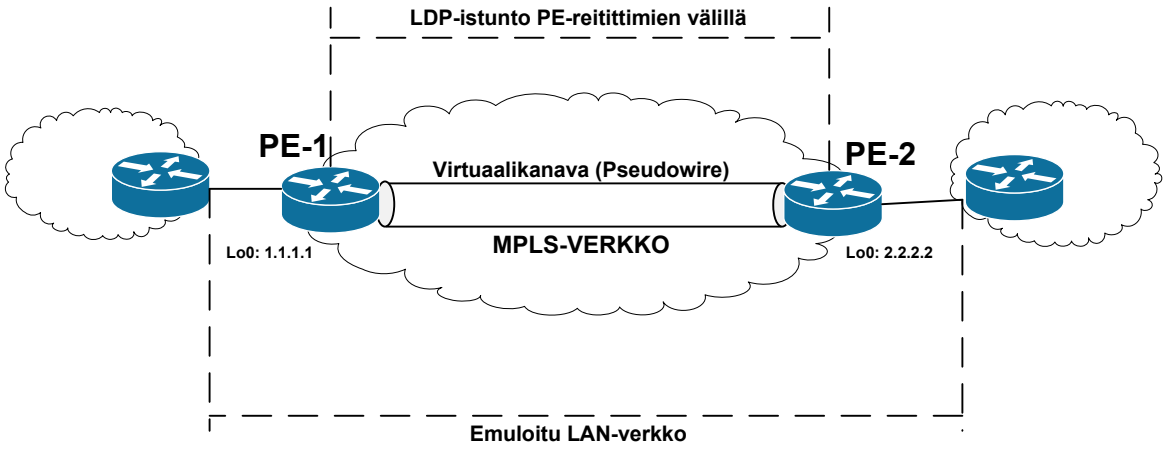
E-LAN-ratkaisu on hieman monimutkaisempi, koska sen avulla voidaan muodostaa eräänlainen virtuaalinen silta kahden toimipisteen välille. Silta toimii kuitenkin kuin

mikä tahansa kytkin Ethernet-verkossa ja sen ansiosta saadaan aikaan yhtenäinen LAN-verkko kahden tai useamman toimipisteen välille. (19)

2.3.1 EoMPLS-tekniikka

EoMPLS (Ethernet over Multiprotocol Label Switching) -tekniikka on osa AToM (Any Transport Over MPLS) -tekniikkaa. AToM puolestaan kuuluu Ethernet Carrierin E-Line-ryhmään ja perustuu MPLS-tekniikkaan lisäten siihen Layer 2 -tason ominaisuuksia. EoMPLS-tekniikan tarkoitus on muodostaa Point-to-Point-yhteys kahden LAN (Local Area Network) -verkon välille MPLS-verkon yli. Minkäänlaista LAN-emulointia ei tapahdu, vaan EoMPLS toimii kahden PE-reitittimen välillä Pseudowiren avulla. Pseudowire on eräänlainen virtuaalikanava, jonka sisällä Ethernet-kehykset kulkevat PE-reitittimeltä toiselle. (4, 416–422)

PE-reitittimen portti asiakkaan suuntaan voi olla joko tavallinen Ethernet-portti tai 802.1Q VLAN -portti, jolloin yhden pseudowiren sisällä voi liikennöidä monta eri VLAN:a samaan aikaan. LDP-protokolla erottaa nämä erilaiset virtuaalikanavat toisistaan tunnisteella. VC Type -tunnisteella erotetaan Ethernet Port - ja Ethernet VLAN -tilat toisistaan. Ethernet Port -tila käyttää VC Type 5 -tunnistetta ja Ethernet VLAN -tila VC Type 4 -tunnistetta. (4, 416–422; 20, 6–7)



Kuva 3. EoMPLS-verkon toimintaperiaate

Kuvassa 3 on esitetty EoMPLS-verkon toimintaa. WAN (Wide Area Network) -yhteys toimii siltana kahden LAN-verkon välillä. PE-reititin lähettää kehyksen kaikille niille PE-reitittimille, jotka kuuluvat samaan Layer 2 VPN:iin. VLAN-tilassa PE-reitittimille merkitykselliset VLAN-merkit (VLAN tag) ovat aina läsnä. Port-tilassa

VLAN:n merkillä ei ole väliä. Vaikka merkkiä ei olisikaan, PE-reititin kuljettaa kehyksen silti toiselle PE-reitittimelle. Port-tila mahdollistaa kokonaisen Ethernet trunk -yhteyden kuljettamisen yhtä virtuaalikanavaa pitkin. (4, 416–422; 20, 6–7)

Vastaanottaessaan Ethernet-kehyksen asiakasverkosta PE-reititin poistaa siitä SFD- (Start of Frame Delimiter) ja FCS (Frame Check Sequence) -tiedot, lisää siihen virtuaalikanavan tunnisteen ja MPLS-liput, minkä jälkeen se lähettää paketin MPLS-verkkoon. Jos Ethernet-kehys on lisäksi merkitty 802.1Q trunk -merkillä, pysyy se kehyksessä. Vastaanottaessaan kuljetetun Ethernet-kehyksen MPLS-verkosta PE-reititin poistaa siitä virtuaalikanavan lipun ja tunnisteen, lisää siihen FCS-tiedot ja tämän jälkeen lähettää kehyksen CE-laitteelle. (4, 416–422)

2.3.2 VPLS-tekniikka

VPLS (Virtual Private Lan Service) kuuluu Carrier Ethernet -ryhmän E-LAN-kategoriaan ja emuloi LAN-verkkoa MPLS-verkon yli käyttämällä virtuaalikanavaa. VPLS-tekniikan avulla palveluntarjoaja luo yhden tai useamman LAN-verkon jokaiselle asiakkaalle. Jokainen näistä LAN-verkoista on täysin yksityinen, joten asiakkaille luodut LAN-verkot eivät ole keskenään tekemisissä millään tavalla. Taustalla toimiva VPLS-tekniikkaa tukeva MPLS-verkko toimii virtuaalisena Ethernet-kytkimenä. (4, 436–441; 21)

VPLS-tekniikka tuli tarpeelliseksi, koska MPLS L3VPN -tekniikka keskittyy IP-tekniikan ympärille. MPLS L3VPN -tekniikan ylitse ei voida kuljettaa muuta kolmannen kerroksen liikennettä. VPLS-tekniikassa Ethernet-kehykset kuljetetaan MPLS-verkon ylitse samalla periaatteella kuin EoMPLS-tekniikassa. EoMPLS-tekniikan ollessa Point-to-Point-tekniikka, on VPLS Point-to-Multipoint-tekniikka, minkä vuoksi VPLS-tekniikan täytyy tukea Broadcast- ja Multicast-kehyksiä. Niiden täytyy kulkea kaikkialle VPLS-verkossa. Emuloidakseen Ethernet-kytkintä täytyy VPLS-tekniikan tukea myös MAC-osoitteiden oppimista ja ikääntymistä. (4, 436–441; 21)

VPLS-tekniikka emuloi Ethernet-kytkimen LAN-toimintoja. VPLS-tekniikalla on seuraavat ominaisuudet:

1. Ethernet-kehyksien välitys

2. Sellaisten Unicast-kehyksien välitys, joilla on tuntematon MAC-osoite

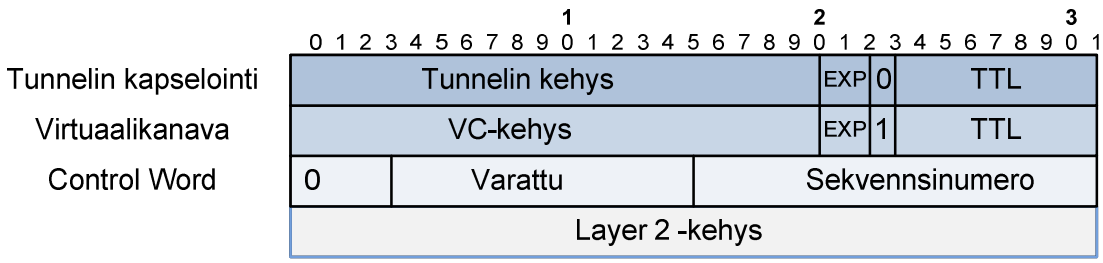
3. Broadcast- ja Multicast-kehyksien toistaminen useampaan kuin yhteen porttiin

4. Silmukoiden ehkäisy

5. MAC-osoitteiden dynaaminen opettelu

6. MAC-osoitteiden ikääntyminen

Kuljetettu kehys on Ethernet-kehys ilman 802.1Q-merkintää. Tämä merkintä poistetaan, ennen kuin kehys lähetetään MPLS-verkkoon. Ethernet-kehykset saavat kaksi MPLS-lippua, ennen kuin ne lähetetään MPLS-verkon yli. Toinen lipuista on VC (Virtual Circuit) -tunnus, jonka avulla tunnistetaan, mihin luotuun virtuaaliseen LAN-verkkoon Ethernet-kehys kuuluu. Tämän lipun päälle tulee vielä normaali MPLS-lippu, jonka avulla paketti löytää perille toiselle PE-reitittimelle MPLS-verkossa. Jos PE-reititin vastaanottaa kehyksen, jossa on tuntematon MAC-osoite, se kopioi sen kaikkiin portteihin, jotka kuuluvat samaan VLANiin. VPLS-tekniikkaa konfiguroidessa täytyy määritellä, mihin VPLS-instanssiin kukin portti tai VLAN kuuluu. PE-reitittimien välillä on virtuaalikanavat, joiden välillä Ethernet-kehykset kulkevat. (4, 436–441; 21)



Kuva 4. Virtuaalikanavan kapselointi

Kuvassa 4 esitetään virtuaalikanavassa kulkevan viestin kapselointi. Jotta PE-reitittimien virtuaalikanavat voitaisiin pitää silmukkavapaina, tarvitaan protokolla, joka estää silmukoiden muodostumisen. STP (Spanning Tree Protocol) -protokolla pitää Layer 2 -topologian silmukkavapaana. On olemassa kuitenkin yksinkertaisempikin mekanismi, jolla tämä onnistuu. VPLS-tekniikkaa käytettäessä PE-reitittimet täytyy

konfiguroida Full Mesh -ajatuksen mukaisesti, eli jokaiselta PE-reitittimeltä täytyy olla virtuaalikanava kaikkiin saman VPLS-instanssin PE-reitittimiin. Tämä mahdollistaa Split-horizon-tekniikan käyttämisen Layer 2 -välityksessä. Split-horizon-tekniikalla tarkoitetaan sitä, että yhdestä virtuaalikanavasta vastaanotettua kehystä ei enää lähetetä muihin virtuaalikanaviin. (4, 436–441; 21)

Kun VPLS-instanssia konfiguroidaan, täytyy kaikki samaan VPLS-instanssiin kuuluvat VPLS-naapurit konfiguroida PE-reitittimelle. Tämän jälkeen PE-reitittimet muodostavat LDP-istunnon keskenään. LDP-istunto mainostaa VC-lippuja ja lähettää signaaleja jokaiseen virtuaalikanavaan. (4, 436–441; 21)

Ethernet-kytkinten tapaan PE-reitittimet tukevat VPLS-verkossa MAC-osoitteiden oppimista ja ikääntymistä. PE-reitittimet huomaavat MAC-lähdeosoitteen vastaanotetuista kehyksistä ja liittävät sen tiettyyn fyysiseen porttiin tai virtuaalikanavaan. Ethernet-kytkimen tapaan MAC-osoitteet poistetaan MAC-taulusta tietyn ajan kuluessa, jos kyseisestä osoitteesta ei tule kehyksiä. MAC-taulu välittää Ethernet-kehykset porteista virtuaalikanaviin ja päinvastoin. (4, 436–441; 21)

Ciscon laitteiden tapauksessa jokaisella MPLS-verkkoon yhteydessä olevalla asiakkaalla on VFI (Virtual Forwarding Instance) -instanssi, jonka avulla reitittimien käyttöjärjestelmä Cisco IOS (Internetwork Operating System) tekee välityspäätöksiä. VFI pitää sisällään mm. PE-reitittimen konfiguroinin, VC-lipun tietoja ja LDP-protokollan tiedon, joka antaa merkkejä virtuaalikanaville. Myös MAC-taulun tiedot löytyvät VFI:stä. (4, 436–441; 21)

3 LAITTEET

Tässä luvussa esitellään työssä käytettyjä verkkolaitteita ja niiden tärkeimpiä ominaisuuksia tämän työn kannalta. Luvussa käsitellään myös verkkolaitteisiin asennettavia moduuleja.

3.1 Cisco Catalyst 3560 -kytkin

Hankitut WS-C3560G-24TS-kytkimet kuuluvat Cisco Catalyst 3560 -sarjaan. Kuva 5 havainnollistaa, miltä kyseinen kytkin näyttää. Kytkimissä on 24 kappaletta Gigabit

Ethernet -portteja ja kuvasta poiketen neljä SFP-moduulipaikkaa joko kupari- tai kuituyhteyttä varten.

Kuva 5. Cisco Catalyst 3560 -kytkin

Catalyst 3560 -kytkimiä oli tarkoitus käyttää simuloimaan asiakkaan verkossa sijaitsevaa Ethernet-kytkintä. 802.1Q trunk -kytkentäisissä verkoissa kytkimen portit jaettiin VLAN:n avulla kolmeen VLAN:iin. Kytkimiin liitettiin työn aikana työasemia, joiden avulla testattiin virtuaalikanavan toimivuutta MPLS-verkon ylitse.

3.2 Cisco 2821 -reititin

Cisco 2821 -reititin on hieman kehittyneempi ja monipuolisempi kuin alemman sarjan 2800-reitittimet. Se tukee EoMPLS-tekniikkaa, jota ei halvemmista 2800-reitittimistä löydy. 2821-reititin on 7604-reitittimen ohella tärkein laite tämän työn kannalta. Laitteessa on kaksi Gigabit Ethernet -porttia reititystä varten ja kaksi moduulipaikkaa moduuleita varten.

Kuva 6. Cisco 2821 -reititin

Kuva 6 havainnollistaa reitittimen ulkonäköä. 2821-reitittimiä oli tarkoitus käyttää työssä CE-reitittiminä C-verkon reunalla eli asiakkaan verkon reunareitittiminä.

3.3 Cisco 7604 -reititin

Työn kannalta tärkein laite on Ciscon 7604 -reititin. Se on modulaarinen laite, johon asiakas voi valita tarpeelliseksi kokemansa moduulit.

Kuva 7. Cisco 7604 -reititin

Kuvasta 7 voi nähdä laitteen etuosassa olevat moduulipaikat sekä vasemmalla olevan moduulipaikan tuulettimille. Hankituissa 7604-reitittimissä oli seuraavat moduulit:

- WS-SUP32-GE-3B Supervisor -valvontamoduuli, joka vastaa laitteen toiminnoista ja ilmoittaa mahdollisista virheistä laitteen toiminnassa. Moduulissa on neljä lediä, jotka kertovat laitteen tilan. Mikäli jokin led palaa punaisena, on siinä osa-alueessa jotain vikaa. Moduulissa on myös yhdeksän Gigabit Ethernet -porttia. Kuvasta 8 nähdään Supervisor-moduulin kahdeksan Ethernet-porttia, jotka tarvitsevat toimiakseen SFP-moduulin. Oikealla oleva Ethernet-portti ei tarvitse SFP-moduulia, vaan se on suoraan käyttövalmis. Tämän portin avulla on helppo päivittää laitteeseen uudempi IOS-järjestelmä.

Kuva 8. WS-SUP32-GE-3B Supervisor –valvontamoduuli

Valvontamoduuli sisältää PFC3B (Policy Feature Card 3B) -kortin sekä MSFC (Multilayer Switch Feature Card) -kortin, joiden avulla valvontamoduulista saadaan tehokas reititin. Vaikka kyse onkin valvontamoduulista, on laite silti tehokkaampi kuin monet halvemmat reitittimet.

- Kaksi 2700 W:n virtalähdettä, jotka toimivat redundanttisesti. Toisen rikkoutuessa toinen syöttää vielä sähköä, joten yksi rikkoutunut virtalähde ei saa laitetta sammumaan. Supervisor-moduuli havaitsee rikkoutuneen virtalähteen ja ilmoittaa siitä varoitusvalolla ja viestillä komentoriville.
- FAN-MOD-4HS-tuuletinmoduuli, joka sijaitsee laitteen kyljessä ja viilentää laitteen komponentteja ja lisämoduuleita. Käytössä laite rasittuu ja lämpenee, joten asianmukainen viilennys on tarpeen. Viileämpänä toimivat laitteet kestävät pidempään. Rikkoutunut tuuletinmoduuli on vaihdettavissa uuteen laitteen ollessa käynnissä, eli laitetta ei tarvitse ajaa alas moduulinvaihdon ajaksi.
- SIP400-lisämoduuli VPLS-tekniikalle, ks. kohta 3.4.

Laitteisiin hankittiin myös Cisco IOS Advanced IP Services -lisenssi, joka on laitteen IOS. Laitteeseen on mahdollista asentaa monia erilaisia linjakortteja ja lisämoduuleja. Reitittimiin asennettiin SIP400-lisämoduuli tukemaan mm. VPLS-tekniikkaa.

7604-reititin sopii moneen tarkoitukseen, kuten verkon reunareitittimeksi ja erityisesti IP/MPLS-reunareitittimeksi. Sopivuutta tukee myös tuki VPLS-tekniikalle. Laitteen lisämoduulit voidaan konfiguroida kahdella tavalla. Konfiguroinnissa voidaan käyttää joko yhtä Supervisor-moduulia ja kolmea linjakorttia tai kahta Supervisor-moduulia ja kahta linjakorttia. Jälkimmäisellä tavalla taataan korkea saatavuus ja redundanttisuus. SimuNet-hankkeen laitteissa käytettiin yhtä Supervisor-moduulia ja yhtä lisämoduulia, koska kyseessä oli laboratorioympäristö.

3.4 Cisco SIP400 -lisämoduuli

SIP400 on lisämoduuli 7600-sarjan reitittimille. Sen avulla reitittimeen saa lisää operaattoritason ominaisuuksia, kuten suuret reititystaulut ja tuen L2VPN-tekniikoille. Työn aikana kävi ilmi, että ainoastaan SIP-kortin avulla on mahdollista toteuttaa VPLS-verkko aliliityntäporttien avulla.

Kuva 9. SIP400 lisäkortti

Kuvan 9 SIP-kortti ei ole aivan täysin samanlainen tässä työssä käytetyn SIP-kortin kanssa, koska SPA (Shared Port Adapter) -versioita on erilaisia ja käyttämässäni mallissa oli kaksi SPA:ta, joissa kummassakin oli viisi porttia. Porttiin liitettiin SFP-moduulit, jotta niistä saatiin toimivia Ethernet-portteja.

3.5 Cisco ASA 5510 -palomuuri

ASA (Adaptive Security Appliance) 5510 on Cisco Systemsin valmistama palomuuri, joka on tarkoitettu pienille ja keskisuurille yrityksille. Tässä työssä ei tarvittu palomuuria, mutta se asennettiin silti samaan aikaan laitekaappiin muiden SimuNet-hankkeen laitteiden kanssa.

3.6 SFP-moduuli

SFP (Small Form-Factor Pluggable) -moduuli on lähetin-vastaanotin, jota käytetään tietoliikennesovelluksissa. SFP-moduuli on samankaltainen GBIC (Gigabit Interface Converter) -moduulin kanssa, mutta sen sisältämä tekniikka on saatu mahtumaan pienempään tilaan, ja siksi se tunnetaan myös nimellä mini-GBIC. Kyseessä on formaatti, jota moni komponenttivalmistaja tukee.

SFP-moduulit on suunniteltu tukemaan SONET- (Synchronous Optical Networking), Gigabit Ethernet -, valokuitu- ja muita tiedonvälitysstandardeja. SFP-moduulista on olemassa monia erilaisia lähetin- ja vastaanotintyyppejä, joista voidaan valita yhteysvälille tietyt edellytykset täyttävä moduulityyppi. Edellytys voi olla esimerkiksi yhteysvälin pituus. Kuparitekniikalla päästään noin 100 metrin pituisiin yhteysväleihin, kun taas kuidulla yhteysväli voi olla jopa kymmeniä kilometrejä. Pitkillä yhteysväleillä voidaan käyttää myös vahvistimia vahvistamaan signaalia. SFP-moduulin tehtävä on muuttaa laitteelta tuleva signaali kupari- tai kuitukaapelissa kulkevaksi signaaliksi.

Kuva 10. Ciscon SFP-kuitumoduuli

Kuvassa 9 on Cisco Systemsin valmistama kuitutekniikkaa tukeva SFP-moduuli ja kuvassa 10 on Ciscon valmistama kuparitekniikkaa tukeva SFP-moduuli. SFP-tekniikasta ei ole olemassa varsinaista standardia, jota kaikkien valmistajien odotetaan noudattavan, vaan tekniikasta on sovittu MSA:n (Multi Source Agreement) mukaisesti. Työssä ilmenneet ongelmat yhteensopivuuksien kanssa johtuivat yleisen standardin puuttumisesta.

Kuva 11. Ciscon 1000BASE-T SFP-moduuli

4 ASENNUKSET

Tässä luvussa käsitellään laitteiden sekä laitekaapin fyysiset asennukset sekä laitteistopäivityksien toteuttamista.

4.1 Laitekaapin asennus

SimuNet-verkon laitteet asennettiin KyAMK:n tietoliikennelaboratorion palvelinhuoneeseen. Laitekaapille raivattiin tilaa palvelinhuoneen perälle, jossa oli jo ennestään kaksi laitekaappia. Näiden kahden laitekaapin laitteet ja verkot on tarkoitus tulevaisuudessa liittää osaksi SimuNet-verkkoa. Laitekaappi asennettiin ensin puoli metriä irti seinästä, koska kaapin takaovi oli mahdollista avata helposti ja mahdollinen huolto olisi helppo suorittaa. Myöhemmin laitekaappi kuitenkin päätettiin siirtää lähemmäs seinää, koska huolto on mahdollista suorittaa yhtä helposti kaapin sivuovien kautta ja kaappi sopii paremmin koko huoneeseen, kun se on lähempänä seinää. Sivuille jätettiin jonkin verran tilaa, jotta ilma pääsisi paremmin vaihtumaan huoneessa.

4.2 Laitteiden asennus laitekaappiin

Laitteet asennettiin kaappiin niiden painon mukaan, eli painavimmat laitteet asennettiin alimmaisiksi ja kevyimmät päällimmäisiksi. 7604-reitittimet olivat painavimpia, joten ne asennettiin alimmaisiksi. Niiden päälle asennettiin 2821-reitittimet, sitten ASA 5510 -palomuurit ja päällimmäisiksi 3560-kytkimet. Kaikkia laitteita ei asennettu aivan toisiinsa kiinni, vaan joidenkin laitteiden välille jätettiin pieni väli konsolikaapeleita ja virtajohtoja varten. Sähkönsyöttö toteutettiin kahdella jatkojohdolla kaapin takana olevasta pistorasiasta. Kaapin yläosaan asennettiin kaksi kytkentärimaa, jotka toimivat yhteyksinä muihin palvelinkaappeihin.

4.3 SIP400-lisämoduulin asennus 7604-reitittimeen

SIP400-lisämoduuli asennettiin 7604-reitittimessä oleviin moduulipaikkoihin. Moduulipaikat on numeroitu ja asennetun moduulin mahdolliset portit saavat numeronsa asennuspaikkansa mukaan. SIP400-moduuli asennettiin kolmanteen moduulipaikkaan. Tällä tavalla Supervisor-moduulin ja SIP400-moduulin väliin jäi tyhjä moduulipaikka.

Asennus oli helppo suorittaa, koska moduulipaikassa oli kiskot, joita pitkin pitkä moduulikortti työnnettiin paikalleen moduulipaikkaan. Tällaisissa asennuksissa on aina pieni staattisen sähkön vaara, mutta varovasti etenemällä vaaroilta vältyttiin. Moduulin fyysisen asennuksen jälkeen reititin ei tarvinnut minkäänlaista erillistä konfigurointia, vaan se tunnisti moduulin itsestään.

4.4 SFP-moduulien asennus

Ciscon 7604-reititin on modulaarinen laite. Sen Supervisor-moduuliin ja SIP-moduuliin voidaan liittää joko kupari- tai kuitutekniikkaa tukevia SFP-moduuleja. Laitteen kanssa oli tarkoitus käyttää Prolabsin valmistamia kuparitekniikkaa käyttäviä SFP-moduuleja, mutta kävikin ilmi, että ne eivät ole yhteensopivia reitittimen SIP-moduulin kanssa. Jotta asiasta voitiin olla täysin varmoja, täytyi SIP400-lisämooduuliin kytkeä vielä muiden valmistajien SFP-moduuleja. Ensimmäiseksi kokeiltiin HP:n kuitutekniikkaa käyttäviä SFP-moduuleja. Liittimien välinen yhteys ei kuitenkaan toiminut lainkaan. Laite ilmoitti tunnistaneensa epäsopivan SFP-moduulin ja kytki sen pois päältä. Hetken aikaa asiaa tutkittuamme selvisi, että Ciscon reitittimet eivät tue automaattisesti muiden valmistajien SFP-moduuleja.

Vielä tarkemmin asiaa selvitettyämme kävi ilmi, että on kuitenkin olemassa salainen komento, jolla Ciscon laite on mahdollista saada toimimaan muiden valmistajien SFP-moduuleilla. Reitittimen saa tukemaan muiden valmistajien SFP-moduuleja syöttämällä **service unsupported-transceiver** -komennon laitteeseen configure terminal -tilassa. Tämän jälkeen HP:n kuitumoduulit alkoivat toimia ja ensimmäinen toimiva yhteys saatiin aikaiseksi SIP400-lisämoduulien välille.

Komento ei kuitenkaan vaikuttanut Prolabsin kuparimoduulien toimintaan ja tästä syystä ne oli pakko palauttaa. Kymen Puhelin antoi lainaksi Ciscon SFP-moduulit. Nämä moduulit toimivat ongelmitta, koska ne olivat Ciscon valmistamia. Kaiken tämän jälkeen 7604-reitittimissä oli kummassakin yksi Ciscon SFP-moduuli ja yksi HP:n SFP-moduuli.

4.5 Kaapelinvedot

Laitekaappiin asennettiin kaksi kytkentärimaa, ja niihin 12 liitintä kumpaankin. Näin SimuNet-verkko on helppo liittää muihin laboratorion testiverkkoihin. Kaapelit vedettiin katossa olevan kaapelikourun kautta. Kaapelointina käytettiin Cat6-kaapelointia.

Kaapelinvedot oli syytä suunnitella tarkasti. Tässä asiassa sain apua tietoliikenneinsinööri Tomi Pahulalta. Kaapelit päätettiin vetää kummastakin palvelinkaapista SimuNet-kaapin kahteen kytkentärimaan. Näin kokonaismääräksi tuli 12 yhteyttä kumpaankin palvelinkaappiin.

4.6 Laitteiden IOS-päivitykset

Ennen kuin uusia laitteita otetaan käyttöön, kannattaa ne ensin päivittää uusimpaan IOS-versioon. Uusin IOS-versio saattaa tuoda mukanaan uusia tekniikoita, joten laitteet on helpompi päivittää ennen asennusta kuin niiden ollessa jo tuotantokäytössä. Tehtaalla asennettu IOS-versio saattaa olla pahimmassa tapauksessa vanhentunut paljonkin ja siitä syystä päivitys saattaa olla paikallaan. Cisco tarjoaa useita erilaisia IOS-versioita asiakkaan tarpeen mukaan ja erilaisille asiakasryhmille. Tuotantoverkoissa kannattaa ensin varmistua siitä, että haluttu IOS-versio on vakaa, eikä siinä esiinny ongelmia. SimuNet-laitteet tulevat laboratoriokäyttöön, joten vakaus ei ole kovin tärkeä asia. Sen vuoksi voitiin valita uusin versio, jossa on eniten ominaisuuksia.

4.6.1 2821-reitittimen IOS-päivitys

Laitteiden saavuttua toimittajalta oli tärkeää ensin varmistaa, että käytettävissä olevat laitteet tukevat EoMPLS-tekniikkaa, ja jos ne eivät tue, onko mahdollisesti uudempaa IOS-versiota saatavissa kyseisille laitteille. Tämä selviää helposti vaikkapa tarkistamalla asia Ciscon Internet-sivuilta. Selvitin asian yrittämällä konfiguroida johonkin reitittimen rajapintaan **xconnect**-käskyn. Jos reititin ei tunnista lainkaan kyseistä käskyä, on miltei varmaa, että laite ei tue EoMPLS-tekniikkaa. Laite saattaa kuitenkin tukea **xconnect**-käskyä, mutta ei kuitenkaan tue EoMPLS-protokollaa. Tästä saattaa selvitä IOS-versiota päivittämällä.

2821-reitittimiin asennettiin uudempi IOS-versio, jotta EoMPLS-tekniikka saatiin käyttöön. Päivitys tehtiin kirjautumalla Ciscon Internet-sivuille ja etsimällä sieltä en-

sin oikea laite ja sen jälkeen vertailemalla eri IOS-versioita. Versioita on olemassa erilaisia eri tarkoituksiin, ja haluttiin versio, jossa olisi mahdollisimman paljon ominaisuuksia. Paljon ominaisuuksia sisältävä IOS vie tietenkin enemmän tilaa ja laitteen muistin määrä täytyi vielä tarkastaa. Lopulta päädyttiin **c2800nm-advipservicesk9-mz.124-11.XJ4** -nimiseen IOS-versioon, koska se sisältää eniten ominaisuuksia.

IOS asennettiin lataamalla ensin asennustiedosto tietokoneelle ja siirtämällä se FTP-palvelimen avulla laitteeseen. Vanhempi IOS piti poistaa laitteen Flash-muistista, ennen kuin uudempi voitiin kopioida Flash-muistille. Laite aloitti uudemman IOS-version asentamisen komennolla **copy tftp flash**. Komennossa määritettiin myös laitteelle tarvittavat tiedot, kuten FTP-palvelimen IP-osoite ja tiedoston nimi. Tämän jälkeen laite käynnistettiin uudelleen.

Ongelmaksi muodostui kuitenkin laitteeseen jäänyt käynnistyskonfiguraatio, joka ei sallinut kirjautua laitteelle enää päivityksen jälkeen. Ongelmasta pääsi eroon käynnistämällä laitteen ROM Monitor -tilaan ja vaihtamalla konfiguraatioregisteriksi 0x2142. Siten laite käynnistyi ilman nykyistä käynnistyskonfiguraatiota, ja se oli mahdollista poistaa muistista. Poistamisen jälkeen konfiguraatiorekisteri vaihdettiin takaisin alkuperäiseksi eli 0x2102:ksi. Tämän jälkeen laite käynnistettiin uudelleen.

4.6.2 7604-reitittimen IOS-päivitys

7604-reitittimien päivitys ei ollut aivan niin yksinkertainen kuin 2821-reitittimien. Laite on modulaarinen, joten täytyi varmistua siitä, että laitteen kaikki osat on varmasti tuettu uudessa IOS-versiossa. Laitteessa on monia eri muisteja, ja IOS-tiedosto pitää siirtää oikeaan paikkaan. IOS päätettiin siirtää /supbootdisk-nimiseen alihakemistoon, sillä siellä sijaitsi laitteeseen esiasennettu IOS. Laitteessa on SIP-lisämoduuli, joka on tärkeää päivittää samalla, kun laitteen IOS päivitetään. Laitteen edellinen IOS-versio täytyi poistaa, ennen kuin asennuksessa voitiin edetä.

Laitteen päivitys aloitettiin samalla tavalla kuin 2821-reitittimien IOS-päivitys. Kannettavalle tietokoneelle tehtiin FTP-palvelin, josta laite hakee uuden IOS-version Flash-muistiinsa.

Show version -komennolla nähdään laitteessa sillä oleva IOS-versio ja **show modules all fpd** -komennolla nähdään SIP400-kortilla sijaitsevan FPD-levykuvan versionume-

ro. FPD-levykuva on SIP400-lisämoduulin oma IOS, ja se tulisi päivittää aina samalla, kun varsinaisen laitteen IOS päivitetään. Päivitysohjeita noudatettiin huolellisesti ja tarkasti, sillä haluttiin välttää kaikki mahdolliset ongelmat. Levykuva kopioitiin Flash-muistiin samaan paikkaan kuin laitteen oikea IOS, jotta laite osaisi päivittää sen automaattisesti käynnistämisen yhteydessä. IOS huomasi käynnistyksen yhteydessä uuden FPD-levykuvan olevan Flash-muistissa, joten IOS päivitti sen automaattisesti entisen tilalle. Levykuvan tiedostonimeä ei saanut vaihtaa, sillä IOS ei käynnistyksen aikana pystyisi löytämään kyseistä tiedostoa, mikäli nimi olisi vaihdettu.

Uuden IOS-version käynnistymisen jälkeen tarkistettiin **show version** -komennolla, että uusi IOS oli varmasti nyt toimintakunnossa. **Show modules all fpd** -komennolla tarkastettiin SIP400-moduulin FPD-levykuvan versio. Se oli kuitenkin jo aiemmin ollut ajan tasalla ja ei näin ollen olisi edes tarvinnut päivitystä.

5 SIMUNET-ALUSTAN TESTAUS EOMPLS-RATKAISULLA

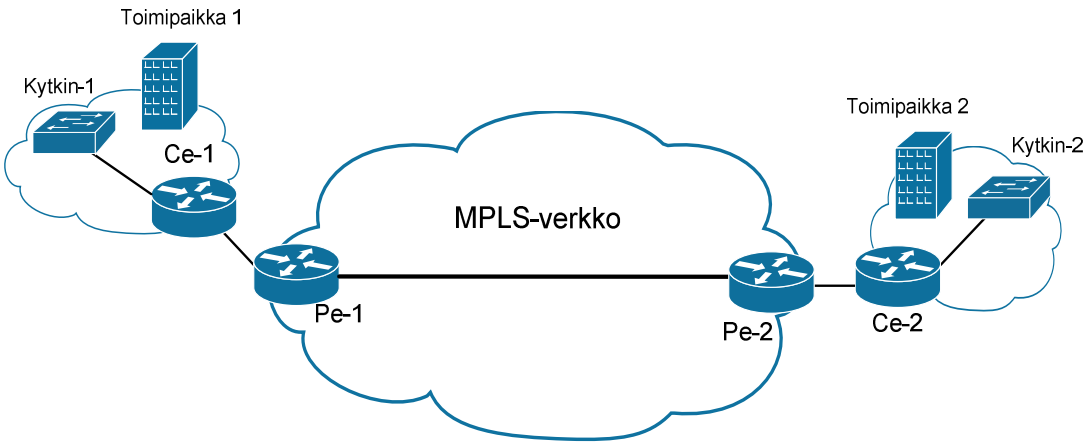
Ensimmäisten laitteiden saavuttua oli mahdollista aloittaa EoMPLS-verkon rakentaminen ja testata laitteiden toimivuus kyseistä tekniikkaa käytettäessä. Tässä vaiheessa fyysisen topologian muodostivat vain 2821-reitittimet ja 3560-kytkimet. EoMPLS-tekniikka ei tarvitse 7604-sarjan laitteita, joten käytännön tutustuminen voitiin aloittaa. Laitteiden sijoittelulla topologiassa ei ollut väliä, koska tekniikka oli tuettu IOS-päivityksen jälkeen kaikissa reitittimissä. Työssä käytetyistä laitteista 7600-reitittimet tukivat EoMPLS-tekniikkaa ilman päivityksiä, mutta 2821-reitittimet tarvitsivat IOS-päivityksen.

Myöhemmin EoMPLS-tekniikkaa kokeiltiin vielä, kun laitteet oli jo asennettu laitekaappiin. Silloin käytettävissä olivat kaikki SimuNet-laitteet. Asioiden selventämiseksi 7604-reitittimistä tehtiin PE-reitittimet. Kahdesta 2821-reitittimestä tehtiin CE-reitittimet ja 3560-kytkimet toimivat eräänlaisina päätelaitteina yhteyden kokeilemista varten. Testitulokset ja topologiat perustuvat siis tähän myöhempään kokeiluun.

5.1 Topologia

EoMPLS-topologian muodostivat kaikki SimuNet-laitteet. Teknologian avulla oli tarkoitus yhdistää kaksi kuvitteellista yrityksen toimipaikkaa toisiinsa Layer 2 -tasolla. Kokeilussa käytettiin EoMPLS-tekniikkaa yhdistämään toimipaikat toisiinsa. Palve-

luntarjoajan reunareitittiminä toimivat 7604-reitittimet ja asiakkaan reunareitittiminä 2821-reitittimet. Kytkiminä ja varsinaisen yhteyden testaajina toimivat 3560-kytkimet.



Kuva 12. EoMPLS-verkko

Kuvasta 12 voi nähdä, miltä kyseisen topologian rakenne näyttää. Tässä topologiassa MPLS-verkon muodostavat pelkästään PE-reitittimet, koska työn aikana SFP-moduuleita ei ollut riittävästi, jotta MPLS-verkkoon olisi voinut sijoittaa P-reitittimen. Tämä ei kuitenkaan vaikuta verkon toimintaan millään tavalla.

PE-reitittimet muodostavat virtuaalikanavan suoraan toistensa välille ilman välissä olevia reitittimiä. Tämän vuoksi MTU (Maximum Transmission Unit) -arvoon ei tarvitse kiinnittää huomiota. Joissain tapauksissa MTU-arvo kasvaa suureksi pakettikytkentäisissä verkoissa suuren verkon ja tarvittavien hyppyjen takia. Tämän vuoksi se täytyy konfiguroida suuremmaksi reitittimien konfiguraatioista. MTU-arvo on suositeltavaa konfiguroida samankokoiseksi kaikissa reitittimissä ongelmien välttämiseksi. Erisuuruiset arvot voivat joissain tapauksissa estää EoMPLS-verkon toiminnan kokonaan.

5.2 EoMPLS-verkon toteutus porttitilassa

Porttikytkentä on helpoin tapa toteuttaa EoMPLS-tekniikkaa käyttävä verkko. Porttitilassa kaikki PE-reitittimen porttiin tuleva liikenne kuljetetaan yhtä virtuaalikanavaa pitkin MPLS-verkon yli. Asiakkaan reunareititin kytketään suoraan palveluntarjoajan reunareitittimeen.

Verkon fyysisen rakentamisen jälkeen konfiguroin kaikkiin laitteisiin toimivan peruskonfiguraation IP-osoitteineen ja reititysprotokollineen. MPLS-verkon sain toimimaan konfiguroimalla **mpls ip** -käskyn reitittimien liityntäportteihin. Tämän jälkeen konfiguroin PE-reitittimien liityntäportin asiakkaaseen päin **xconnect**-käskyllä. **Xconnect**-käsky luo PE-reitittimien välisen virtuaalikanavan reitittimien välille. Käskyn avulla reitittimet kuljettavat Ethernet-kehykset virtuaalikanavan yli. Virtuaalikanava tarvitsi oman tunnisteensa (VCID), jonka tässä tapauksessa määrittelin VCID 2000:ksi.

5.3 EoMPLS-verkon toteutus VLAN-tilassa

Porttikytkentä on mahdollista muuntaa 802.1Q trunk -yhteydeksi. Asiakkaan ja palveluntarjoajan välillä oleva yhteysväli konfiguroidaan 802.1Q trunk -tilaan, jolloin monta VLANia voi liikennnöidä saman virtuaalikanavan kautta MPLS-verkon yli. Näin saadaan kuljetettua koko 802.1Q trunk virtuaalikanavan avulla asiakkaan toimipisteiden välillä.

Tässä kytkennässä pohjana käytettiin aiempaa porttikytkentää. Erona aiempaan kytkentään on se, että CE-laitteissa käytetään aliliityntäportteja, joissa jokaisessa kulkee yksi VLAN. Nämä VLANit kulkevat PE-reitittimille, joissa ne erotellaan VLAN-rajapintoihin. VLAN-rajapinnassa käytetään samaa **xconnect**-käskyä kuin aikaisemmin porttitilassa luomaan PE-reitittimien välille virtuaalikanavat.

Kaikki VLANit kulkevat saman VCID-tunnisteen alla, mutta niistä jokainen voidaan myös konfiguroida kulkemaan omaa virtuaalikanavaa pitkin. Tämän etu on se, että jokainen virtuaalijohdin voi kulkea eri reittejä pitkin MPLS-verkon yli. Siten on mahdollista tasata liikenteen määrää suurissa verkoissa verkon osien välillä ja vähentää liikennöinnistä tiettyihin verkon osiin aiheutuvaa kuormitusta.

5.4 EoMPLS-verkon toiminnan testaus

Testitulokset on saatu verkon ollessa porttitilassa. Verkon toiminnan testaus aloitettiin varmistamalla, että konfiguroitu virtuaalikanava on varmasti UP-tilassa. Se tarkistettiin kirjoittamalla **show mpls l2transport vc 2000** -komento toisen PE-laitteen komentoriville.

```
PE-2#show mpls l2transport vc 2000

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1/1          Ethernet                   10.1.1.1        2000       UP
```

Kuva 13. Virtuaalikanavan 2000 tila

Käsky antoi kuvan 13 mukaisen tulosteen. Tulosteesta käy ilmi vastaanottavassa päässä olevan PE-laitteen IP-osoite sekä virtuaalikanavan tila.

```
PE-2#show mpls l2transport vc 2000 detail
Local interface: Gi1/1 up, line protocol up, Ethernet up
  Destination address: 10.1.1.1, VC ID: 2000, VC status: up
    Output interface: Gi3/0/3, imposed label stack {16 16}
    Preferred path: not configured
    Default path: active
    Next hop: 172.16.0.3
  Create time: 01:07:20, last status change time: 01:04:56
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.3(LDP Id) -> 10.1.1.1
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 16, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 461, send 460
    byte totals:   receive 49253, send 49189
    packet drops:  receive 0, seq error 0, send 0
```

Kuva 14. Virtuaalikanavan 2000 statistiikat

Kuvasta 14 nähdään virtuaalikanavan 2000 statistiikat. Kuvassa kohta **VC statistics** kertoo virtuaalikanavassa liikkuneiden pakettien ja tavujen määrän. Liikkuneiden pakettien perusteella voidaan olettaa, että virtuaalikanava on konfiguroitu oikein.

```
PE-1#show mpls l2transport bind
  Destination Address: 10.1.1.3,  VC ID: 2000
    Local Label:  16
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 0,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

Kuva 15. Virtuaalikanavan nidos ja lipputiedot

Kuva 15 kertoo virtuaalikanavan lipputiedot ja pääteosoitteen virtuaalikanavan toisessa päässä. Point-to-Point-yhteyden ollessa kyseessä liput eivät pääse hyppyjen takia muuttumaan ollenkaan.

Olin kiinnostunut kokeilemaan CDP:n (Cisco Discovery Protocol) toimintaa EoMPLS-verkossa ja päätin kokeilla, mitä käsky **show cdp neighbor** antaa tulosteeksi. CDP on OSI-mallin toisella kerroksella toimiva Ciscon kehittämä protokolla, jonka avulla suoraan toisiinsa kytketyt Cisco-laitteet jakavat itsestään tietoa toisilleen.

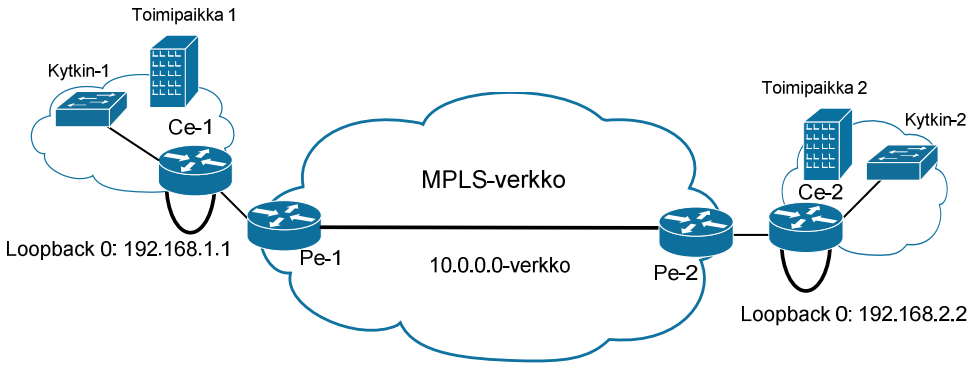
```
Ce-2#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Ce-1             Gig 0/0            148         R S I     2821     Gig0/0
```

Kuva 16. CDP:n toiminta EoMPLS-verkossa

Kuvassa 16 esitetystä käskyn tulosteesta voi päätellä, että CE-laitteiden välissä oleva EoMPLS-verkko on läpinäkyvä CE-laitteille. Näin ollen laitteet olettavat olevansa suoraan yhteydessä toisiinsa. Kokeilin käskyä kuitenkin vain porttitilassa, joten VLAN-tilassa CDP saattaa käyttäytyä eri tavalla.

Lopuksi oli vuorossa Ping-testi toimipaikkojen verkkojen välillä. Toimipaikoissa oli käytössä erilaiset aliverkon osoitteet, ettei Ping-testi onnistuisi vahingossa.



Kuva 17. EoMPLS-verkon Ping-testaus

Kuvassa 15 on havainnollistettu verkon konfigurointi testauksen aikana. Laitteiden välillä oleva EoMPLS-verkko käytti osoitteinaan 10.0.0.0 aliverkon osoitteita, kun taas toimipaikkojen verkot käyttivät 192.168.0.0 aliverkon osoitteita. 192.168.0.0 aliverkon osoitteet konfiguroitiin CE-laitteiden Loopback-osoitteiksi.

Oikein toimiakseen täytyi Ping-testinä käyttää Extended Ping -testiä. Siinä voidaan konfiguroida lähettäjän IP-osoite ja käyttää Loopback 0 -osoitetta. Ilman tätä konfigurointia Ping ei tulisi perille oikeaan paikkaan eikä se lähtisi oikeasta osoitteesta.

```
Ce-2#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Extended commands [n]: y
Source address or interface: 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Kuva 18. Ping-testi Loopback-osoitteiden välillä

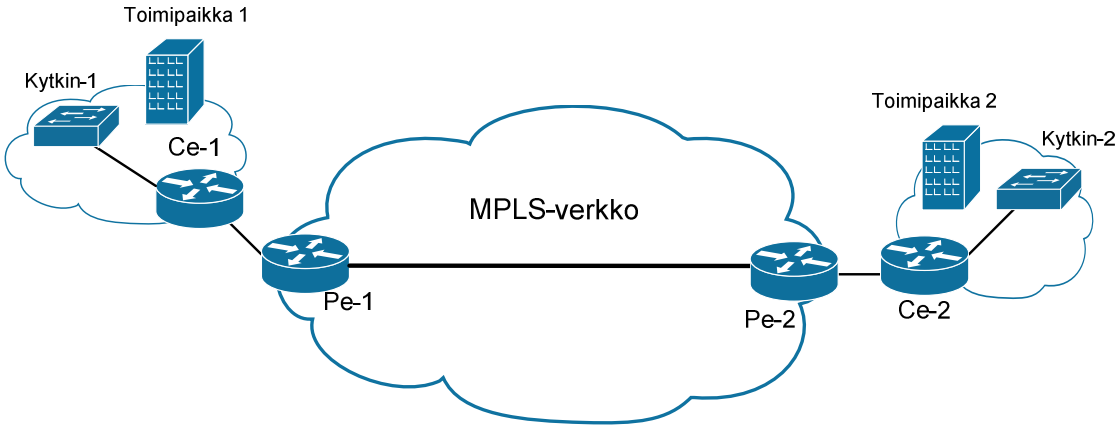
Kuten kuvasta 18 nähdään, Ping-testi toimi oikein ja laitteet pystyivät kommunikoimaan keskenään EoMPLS-verkon yli. Tästä voidaan päätellä, että EoMPLS-verkko oli toimintakunnossa.

6 SIMUNET-ALUSTAN TESTAUS VPLS-RATKAISULLA

VPLS-verkko tarvitsi 7604-reitittimet PE-reitittimiksi MPLS-verkon laidalle, koska ainoastaan näissä laitteissa oli tuki VPLS-tekniikalle. 7604-reitittimien välissä oleva MPLS-verkko voi kuitenkin koostua laitteista, jotka eivät tue VPLS-tekniikkaa. P-reitittimeksi kelpaa siis 2821-reititinkin. P-reititin on vain välittäjän roolissa eikä siis osallistu varsinaiseen VPLS-tekniikkaan, vaan toimii pelkästään IP/MPLS-tasolla pakettien ohjailijana ja kytkijänä.

6.1 Topologia

VPLS-topologia muistutti EoMPLS-verkon topologiaa ja olisi voinut olla myös kokonaan samanlainen, mutta Prolabsin SFP-liittimet lähetettiin takaisin niiden ostopaikkaan, koska ne eivät toimineet toivotulla tavalla.



Kuva 19. VPLS-topologia

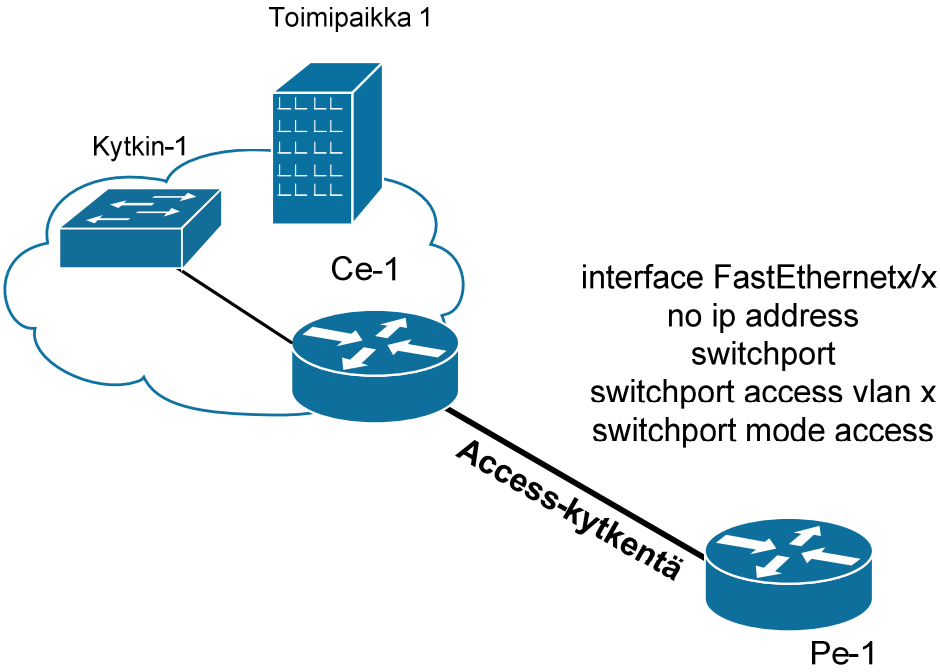
Kuvasta 19 nähdään, että topologiaa jouduttiin muuttamaan ja MPLS-verkko pienentyi hieman. Verkosta poistettiin P-reititin kokonaan, eli PE-reitittimien välille muodostui suora Point-to-Point-yhteys. Se ei kuitenkaan vaikuttanut millään tavalla VPLS-tekniikan tarkasteluun.

VPLS-verkon käyttötarkoitus tai sen vahvuus ei tule täysin esille tämän topologian myötä, mutta se antaa kuitenkin kuvan siitä, kuinka VPLS-verkko toimii. VPLS-tekniikan todelliset ominaisuudet näkyvät kunnolla vasta sitten, kun toimipaikkoja on vähintään kolme. Kolmen eri toimipaikan välille voidaan konfiguroida virtuaalikana-

vat, jolloin verkko toimii kuten oikea Layer 2 -verkko Split Horizon -tekniikka mukaan lukien.

6.2 Access-kytkentä

Access-kytkentä on yksinkertaisin VPLS-verkon konfiguraatio. Access-kytkennässä PE-reitittimen portti asiakkaan suuntaan konfiguroidaan kytkinportiksi. Tämän lisäksi porttiin liitetään sisäinen VLAN-merkki (tag).



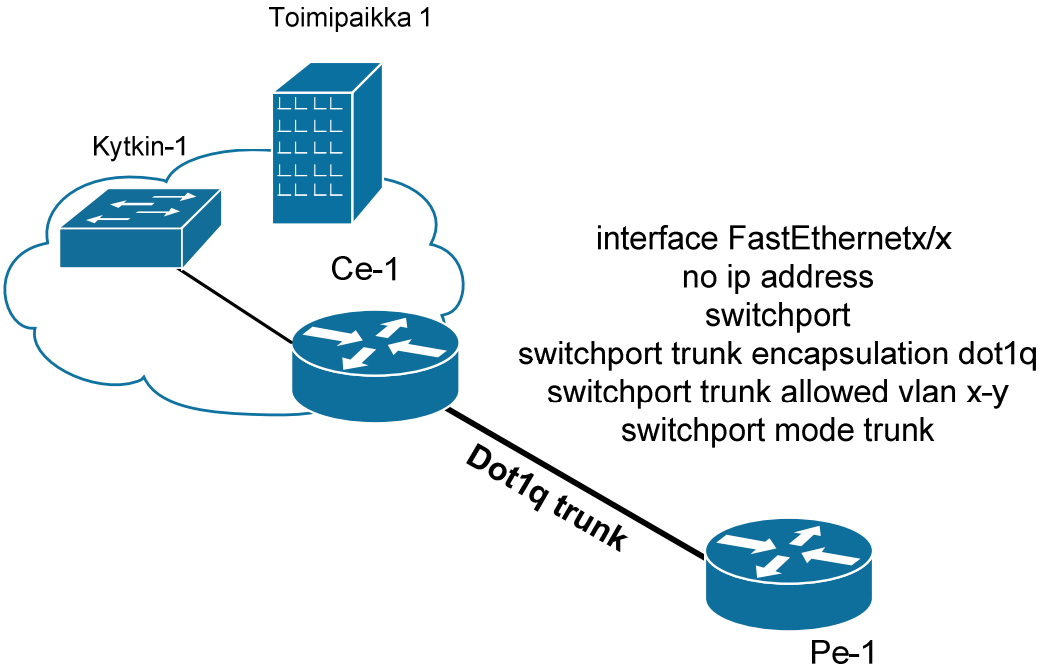
Kuva 20. Access-kytkentäkonfiguraatio

Kuvasta 20 nähdään PE-reitittimen konfiguraatio asiakkaan CE-reitittimen suuntaan. Access-kytkentä on identtinen tavallisen siltauskytkennän kanssa. Vain merkitsemättömät Ethernet-paketit lähetetään ja vastaanotetaan Layer 2 -tason kytkinportissa. Ethernet-paketin otsikko lähetetään muokkaamattomana virtuaalikanavan ylitse.

6.3 802.1Q trunk -kytkentä

802.1Q trunk -kytkentä toimii VPLS-tekniikassa samankaltaisesti kuin EoMPLS-tekniikassa. Ero on lähinnä virtuaalikanavan konfiguroinnissa. Konfiguroitaessa Layer 2 -tason kytkinportti trunk-tilaan VPLS-verkossa VLAN-merkki kartoittaa CE-reitittimeltä saadut paketit siltatoimialueeseen.

Layer 2 -tason kytkinportin rajapinta ei tue konfiguroitavaa palvelua rajoittavaa VLAN-merkkiä. Sen vuoksi VLAN-merkin täytyy täsmätä sisäisen siltatoimialueen VLAN-merkkiin, joka on annettu VPLS-asiakkaalle. Eri VPLS-asiakkaiden liikennöinti Layer 2 -tason kytkinportin yli on mahdollista, koska trunk-tila tukee moninkertaisia VLAN-merkkejä.



Kuva 21. 802.1Q trunk -konfiguraatio

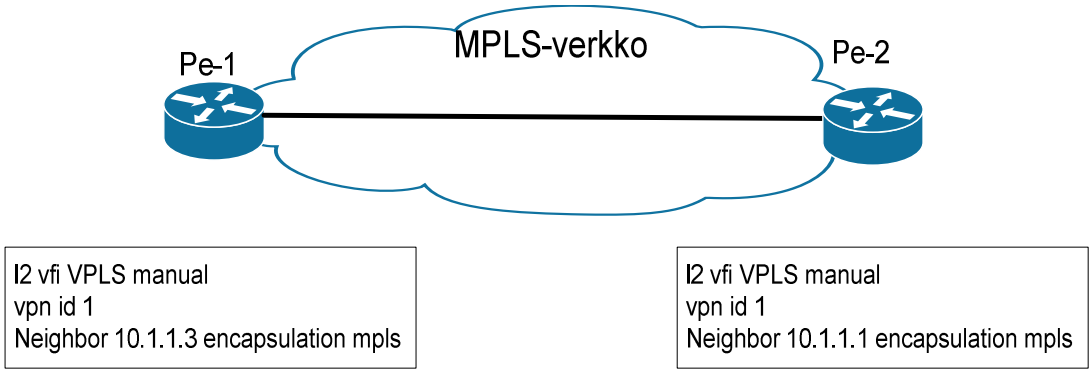
Kuvassa 21 asiakkaan ja palveluntarjoajan välille on konfiguroitu trunk-tila. Trunk-tilassa PE-reititin poistaa palvelua rajoittavan VLAN-merkin Ethernet-paketin otsikosta ennen virtuaalikanavan kapseloinnin lisäämistä. Toiseen suuntaan kuljettaessa PE-reititin lisää sisäisen VLAN-merkin Ethernet-paketin kehykseen sen jälkeen, kun virtuaalikanavan kapselointi on poistettu virtuaalikanavapaketista.

PE-reitittimen rajapinta asiakkaan suuntaan konfiguroidaan asettamalla portti ensin kytkinportiksi. Sen jälkeen porttiin konfiguroidaan 802.1Q trunk -kapselointi, mikä mahdollistaa monen VLANin liikennöimisen yhtä linjaa pitkin. Viimeiseksi määritellään sallitut VLANit, jotka voivat liikennöidä trunk-linjaa pitkin. Tämä ei ole pakollista, mutta se on suositeltavaa, sillä se auttaa pitämään verkon järjestyksessä ja vähentää mahdollisten ongelmien määrää.

6.4 VFI-instanssin konfigurointi

Konfiguroitaessa AToM- tai L2TPv3-ratkaisuja virtuaalikanavan osuus konfiguroinnista tehdään verkkoon liitettävän osan konfigurointitilassa. Tämä osa voi olla esimerkiksi VLAN. Esimerkiksi PPP (Point-to-Point Protocol) ja HDLC (High-Level Data Link Control) käyttävät rajapintatilaa virtuaalikanavien konfigurointiin. Tämä rakentaa epäsuorasti yhteyden verkkoon liitettävän osan (toimipaikan) ja virtuaalikanavan välillä.

VPLS-tekniikka rakentaa monesta moneen (many-to-many) -yhteydet jokaiselle VPLS-toimialueelle. Virtuaalikanavan osuus konfiguroinnista sisältää VFI-instanssin konfiguroimisen, joka puolestaan sisältää tiedot kyseessä olevan toimialueen virtuaalikanavista ja niihin liittyvistä asetuksista.



Kuva 22. VFI-instanssin konfigurointi

Kuvasta 22 nähdään PE-reitittimien VFI-instanssin konfiguraatio. VFI tarvitsee VPN ID -tunnisteen, jotta se voidaan tunnistaa koko VPLS-verkossa. Työssä on annettu virtuaalikanavalle nimeksi **VPLS** ja VPN ID -tunnisteeksi numero **1**. Lisäksi VFI-instanssiin lisättiin kaikki samaan toimialueeseen kuuluvien PE-laitteiden IP-osoitteet, eli tässä tapauksessa Loopback-osoitteet.

Viimeiseksi VFI-instanssi konfiguroitiin VLAN-rajapintaan käskyillä: **interface vlan 111, xconnect vfi VPLS.** Xconnect vfi -käsky viimeistelee many-to-many-yhteyden.

6.5 VPLS-verkon testaus

Aluksi testivuorossa oli Access-kytkennöillä toteutetun VPLS-verkon testaus. Se aloitettiin kuvan 23 perusteella katsomalla VPLS-instanssin peruskonfigurointi. Käsky **show vfi vpls** tulosti kyseisen virtuaalikanavan tiedot.

```
PE-2#show vfi name vpls

Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: vpls, state: up, type: multipoint
  VPN ID: 1
  Local attachment circuits:
    Vlan111
  Neighbors connected via pseudowires:
  Peer Address     VC ID         S
  172.16.1.1       1             Y
```

Kuva 23. VPLS-verkon virtuaalikanava

Jostain syystä virtuaalikanavan toisessa päässä sijaitseva PE-laite näkyi kyseisen laitteen MPLS-verkossa käyttämällä IP-osoitteella 172.16.1.1. Tilanne ei muuttunut, vaikka konfiguroin LDP-protokollan käyttämään laitteeseen konfiguroitua Loopback-osoitetta. Toisissa tulosteissa laite kuitenkin näkyi Loopback-osoitteensa avulla. Toinen PE-laitteista näytti Loopback-osoitteen kaikissa tulosteissa, ja nämä kaksi reititintä konfiguroitiin täsmälleen samanlaisesti. Osoitteella ei kuitenkaan ollut vaikutusta VPLS-verkon toiminnan kannalta. Verkon vianselvityksen kannalta on kuitenkin parempi, kun laitteet käyttävät niille asetettuja Loopback-osoitteita.

```
PE-1#show mpls l2transport summary
Destination address: 10.1.1.3, total number of vc: 1
  0 unknown, 1 up, 0 down, 0 admin down, 0 recovering, 0 standby
  1 active vc on MPLS interface Gi3/0/0
```

Kuva 24. Virtuaalikanavan tila

Kuva 24 kertoo käytössä olevien virtuaalikanavien määrän ja niiden tilan. Virtuaalikanava ei noussut heti toimintakuntoon. Vika oli kuitenkin yhdessä puuttuvassa käskyssä. Tässä tapauksessa virtuaalikanava on saatu toimintakuntoon.

```
PE-1#show mpls l2transport vc 1 detail
Local interface: VFI vpls VFI up
  Interworking type is Ethernet
  Destination address: 10.1.1.3, VC ID: 1, VC status: up
    Output interface: Gi3/0/0, imposed label stack {16}
    Preferred path: not configured
    Default path: active
    Next hop: 172.16.1.2
  Create time: 01:46:12, last status change time: 00:04:26
  Signaling protocol: LDP, peer 10.1.1.3:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.3
    MPLS VC labels: local 17, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    VC statistics:
    packet totals: receive 274, send 228
    byte totals:   receive 25788, send 22804
    packet drops:  receive 0, seq error 0, send 0
```

Kuva 25. Virtuaalikanavan tarkemmat tiedot

Kuvassa 25 on virtuaalikanavan tarkemmat tiedot. Näistä tiedoista selviää LDP-protokollan käyttämä IP-osoite Hello-paketeissa, joka on 10.1.1.1. Tämä on siis hieman ristiriidassa kuvassa 24 olevan IP-osoitteen kanssa. Tiedoista selviää myös, kuinka monta pakettia virtuaalikanavassa on liikkunut siitä asti, kun se on ollut toiminnassa. Tämän perusteella voidaan todeta, että kuvan 24 IP-osoitteella ei ole vaikutusta virtuaalikanavan tilaan tai sen sisällä kulkevaan liikenteeseen.

```
PE-1#show mpls l2transport bind
  Destination Address: 10.1.1.3,  VC ID: 1
    Local Label:  17
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: Ethernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

Kuva 26. VPLS-virtuaalikanavan nidos

Kuvasta 26 selviää virtuaalikanavan käyttämät lippunumerot eli nidokset MPLS-verkossa sekä MTU:n koko.

```
PE-1#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     10.1.1.3/32      0             Gi3/0/0   172.16.1.2
17     No Label      l2ckt(1)         13587         none     point2point
```

Kuva 27. MPLS-lippujen numerot ja siirtomäärät

Kuva 27 kertoo MPLS-taulussa olevien lippujen kytkemiseen liittyvät tiedot. Lippu numero 17 edustaa varsinaista virtuaalikanavaa. Siirtomäärästä voidaan todeta, että tavuja on kytketty virtuaalikanavan kautta 13587 kappaletta. Tässäkin tapauksessa virtuaalikanava toimii oikealla tavalla eli kuljettaa liikennettä MPLS-verkon läpi.

VPLS trunk -konfiguraation testaus

Kuvasta 28 voidaan todeta, kuinka VPLS trunk -konfiguraatiossa PE-laitteisiin konfiguroitiin kolme erilaista VFI-instanssia, joista jokainen piti sisällään yhden VLANin. Tarkoitus oli siis liikennöidä asiakkaan toimipaikasta 1 toimipaikkaan 2 kolmella eri VLANilla. Nämä VLANit olivat 111, 222 ja 333. Jokaisella näistä VLANeista on oma VPN ID -tunnisteensa sekä nimi, jolla on merkitystä vain PE-laitteelle itselleen VFI-instanssien erottelemiseksi.

```
PE-1#show vfi

Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: vpls, state: up, type: multipoint
  VPN ID: 1
  Local attachment circuits:
    Vlan111
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  10.1.1.3         1            Y

VFI name: vpls2, state: up, type: multipoint
  VPN ID: 2
  Local attachment circuits:
    Vlan222
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  10.1.1.3         2            Y

VFI name: vpls3, state: up, type: multipoint
  VPN ID: 3
  Local attachment circuits:
    Vlan333
  Neighbors connected via pseudowires:
  Peer Address     VC ID        S
  10.1.1.3         3            Y
```

Kuva 28. Trunk VPLS -konfiguraation virtuaalikanavat

```
PE-1#show mpls l2transport vc 3 detail
Local interface: VFI vpls3 VFI up
  Interworking type is Ethernet
  Destination address: 10.1.1.3, VC ID: 3, VC status: up
    Output interface: Gi3/0/0, imposed label stack {19}
    Preferred path: not configured
    Default path: active
    Next hop: 172.16.1.2
  Create time: 00:26:10, last status change time:
00:05:37
  Signaling protocol: LDP, peer 10.1.1.3:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.3
    MPLS VC labels: local 19, remote 19
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 327, send 319
    byte totals:   receive 26800, send 26304
    packet drops:  receive 0, seq error 0, send 0
```

Kuva 29. vpls3-virtuaalikanavan tiedot

Kuvassa 29 on otettu tarkasteluun virtuaalikanava 3, joka kuului VLANiin 333. Toimipaikkojen Ethernet-kytkimiin lisättiin työasemat ja ne liitettiin kytkimiin. Työasemille annettiin IP-osoitteet eri osoiteavaruudesta, jotta Ping-testi ei onnistuisi millään tavalla vahingossa. Kytkimen portti oli liitetty VLANiin 333. Kuvasta voi todeta, että virtuaalikanavan sisällä liikkuu paketteja. Samalla tehtiin Ping-testi työasemien välillä. Työasemat pystyivät lähettämään pakettinsa perille ja saivat vastauksen.

```
PE-1#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     10.1.1.3/32      0             Gi3/0/0   172.16.1.2
17     No Label      l2ckt(1)         0             none     point2point
18     No Label      l2ckt(2)         0             none     point2point
19     No Label      l2ckt(3)         30900         none     point2point
```

Kuva 30. MPLS-lippujen numerot ja siirtomäärät

Kuvasta 30 nähdään, että jokaisella VPLS-virtuaalikanavalla on omat tietonsa MPLS-taulussa. Kolmannessa VPLS-instanssissa on tavuja kytketty lipun avulla 30 900 kappaletta. Tässä vaiheessa olin kokeillut liikennöimistä VLAN 333:ssa kahden toimipisteen välillä kytkimiin kytkettyjen työasemien avulla. Kummassakin toimipisteessä kytkinten portti oli konfiguroitu VLANiin 333. Muut VLANit näyttävät vielä nollaa,

sillä niiden kautta ei ole liikennöity. Liikennöinti VLAN 333:n kautta kuitenkin osoitti, että tiedonsiirto on mahdollista VPLS-verkon yli.

Lopuksi kokeilin tehdä PE-laitteista läpinäkyviä CDP-protokollalle, jotta CE-reitittimet näkisivät suoraan toisensa eivätkä PE-laitteita. Käskyn **show cdp neighbor** syöttäminen kertoi, että CE-laittteen viereinen laite on PE-reititin. Käyttämällä käskyjä **l2protocol-tunnel cdp** ja **no cdp enable** asiakkaaseen päin olevassa rajapinnassa oli tarkoitus saada PE-laitteet läpinäkyviksi samalla tavalla kuin aiemmin EoMPLS-tekniikan kanssa. Käskyjen syöttämisen jälkeen CE-laite ei kuitenkaan nähnyt toisessa toimipisteessä olevaa CE-laitetta. Tähän en kyennyt löytämään minkäänlaista ratkaisua. VPLS-virtuaalikanava tuntui kuitenkin toimivan oikealla tavalla.

MAC-osoitetauluja tutkimalla olisi saattanut selvitä syy CDP-protokollan toimimattomuudelle. PE-laitteen MAC-osoitetauluja tutkimalla olisi ehkä saanut tietää, onko PE-laite saanut tietää kaikki virtuaalikanavan kautta kulkevien laitteiden MAC-osoitteet.

7 YHTEENVETO

Työn alussa oli tarkoitus liittää laitteiden etäkäytön toteutus mukaan työhön, mutta sopivien laitteiden puuttuessa juuri sillä hetkellä päätettiin osio jättää tämän työn ulkopuolelle. Työssä oli mielestäni silti tarpeeksi tekemistä ja tutkimista, vaikka tätä tavoitetta ei työssä saavutettukaan.

Laitteiden fyysisessä asennuksessa ei tullut vastaan vakavia ongelmia. SFP-moduulien yhteensopimattomuus aiheutti hieman päänvaivaa, koska testitapaustutkimuksen verkkotopologiat täytyi suunnitella uudelleen pienemmälle laitemäärälle. Pienempi laitteiston kokonaismäärä puolestaan latisti hieman verkon monimutkaisuutta eikä ehkä antanut todellista kuvaa tuotantoverkosta. Loppujen lopuksi palveluntarjoajan tai Internet-operaattorin tuotantoverkko ei koostu pelkästään IP/MPLS-tekniikasta, vaan vain tietty osa tietoverkosta saattaa olla toteutettu kyseistä tekniikkaa käyttäen.

Muutoin työlle asetetut tavoitteet saatiin täytettyä. Testitapaustutkimus oli onnistunut ja täytti työlle asetetut tavoitteet ja odotukset. VPLS-tutkimuksessa CDP-protokollan käyttäytymisen tutkiminen ei onnistunut toivotulla tavalla. Olin kuitenkin tutkinut sitä työssä omasta mielenkiinnostani, eikä sillä ollut käytännössä merkitystä lopputuloksen

kannalta. Työn tuloksena syntyi toimiva SimuNet-verkko tietoliikennelaboratorion palvelinhuoneeseen ja työn aikana tehtyä testitapaustutkimusta on mahdollista käyttää pohjana tulevissa SimuNet-verkkoa koskevissa töissä.

Työssä ei käsitelty VPLS-tekniikkaa kovinkaan syvällisesti, vaan tarkoituksena oli alun perin tutkia SimuNet-laitteiden soveltuvuutta VPLS-tekniikalle ja saada aikaan toimiva VPLS-ratkaisu SimuNet-verkon laitteilla. Tämä tavoite työssä myös saavutettiin. VPLS-tekniikan hyvänä puolena voi nähdä mahdollisuuden ohjata liikennettä monia eri kulkureittejä pitkin verkossa. Tämän avulla lisätään verkon redundanttisuutta, mikä on nykypäivänä tärkeää palveluntarjoajille.

Kehitysideoita jatkoa ajatellen jäi jonkin verran. Esimerkiksi H-VPLS (Hierarchical Virtual Private LAN Service) -tekniikan tutkiminen ja toteuttaminen SimuNet-laitteilla olisi mielenkiintoinen tarkastelun ja tutkimisen kohde. H-VPLS-tekniikan topologia eroaa aika paljon VPLS-tekniikan vastaavasta. Toinen mielenkiintoinen implementointi olisi QoS (Quality of Service) -palvelun lisääminen VPLS-verkkoon. Tämän tekniikan toteuttamisen SimuNet-verkkoon pitäisi olla mahdollista Ciscon 7604-reitittimeen asennetun SIP400-lisämoduulin ansiosta.

Työssä tutkittuun Point-to-Point-tyyliseen EoMPLS-tekniikkaan verrattuna VPLS-tekniikka on kuitenkin jonkun verran monimutkaisempi toteuttaa ja ottaa käyttöön. EoMPLS-tekniikkaa puoltaa helppo käyttöönotto, mutta on kuitenkin erityisen tärkeää suunnitella verkko tarkasti ennen varsinaista käytännön toteutusta. Huolimaton EoMPLS- tai VPLS-tekniikan käyttö voi vaikeuttaa vianpaikannusta ja saattaa helposti tuhota verkon rakenteellisen toteutuksen.

LÄHTEET

1. Kettunen M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana, Tutkimusjulkaisu 2010, Kymenlaakson ammattikorkeakoulun julkaisuja, Sarja B. Saatavissa: http://papaya.tlt.kyamk.fi/~amake/SimuNet/SimuNet%20artikkeliv6a.pdf [viitattu 15.1.2010]

2. McDysan, D. & Paw, D. 2002. ATM & MPLS theory & application: foundations of multi-service networking. The McGraw-Hill Companies.

3. Broadband Forumin verkkosivut. Saatavissa: http://www.broadband-forum.org/about/forumhistory.php [viitattu 20.10.2009].

4. Ghein, D. L. 2007. MPLS Fundamentals. Cisco Press.

5. Rosen, E., Viswanathan, A. & Callon, R. 2001. Multiprotocol Label Switching Architecture. RFC 3031. Saatavissa: http://www.ietf.org/rfc/rfc3031.txt [viitattu 20.9.2009]

6. Bates, R. J. 2000. ATM and frame relay internetworking. McGraw-Hill.

7. Bates, R. J. 2000. Frame relay. McGraw-Hill.

8. Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T. & Conta, A. 2001. MPLS Label Stack Enconding RFC 3032. Saatavissa: http://www.ietf.org/rfc/rfc3032.txt [viitattu 25.9.2009]

9. Guichard, J., Faucheur, F. L. & Vasseur, J. P. 2007. Definitive MPLS Network Designs. Cisco Press.

10. Andersson, L., Doolan, P., Feldman, N., Fredette, A. & Thomas, B. 2001. LDP Specification. RFC 3036. Saatavissa: http://www.ietf.org/rfc/rfc3036.txt [viitattu 1.10.2009]

11. Cisco Systems. MPLS / Tag Switching. Saatavissa: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/MPLS_Tag-Switching.html [viitattu 7.12.2009]

12. Cisco Systems. Cisco Express Forwarding Overview. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdcef.html [viitattu 15.10.2009]

13. Baker, F. 1995. Requirements for IP Version 4 Routers. RFC 1812. Saatavissa: http://www.ietf.org/rfc/rfc1812.txt [viitattu 20.10.2009]

14. Cisco Systems. Routing Basics Saatavissa: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Routing-Basics.html [viitattu 7.12.2009]

15. Rekhter, Y., Li, T. & Hares, S. 2006. A Border Gateway Protocol 4 (BGP-4). RFC 4271. Saatavissa: http://www.ietf.org/rfc/rfc4271.txt [viitattu 21.10.2009]

16. Moy, J. 1998. OSPF Version 2. RFC 2328. Saatavissa: http://www.ietf.org/rfc/rfc2328.txt [viitattu 24.10.2009]

17. Coltun, R. & Fuller, V. 1994. The OSPF NSSA Option. RFC 1587. Saatavissa: http://www.ietf.org/rfc/rfc1587.txt [viitattu 1.12.2009]

18. Gleeson, B., Lin, A., Heinanen, J., Armitage, G. & Malis, A. 2000. A Framework for IP Based Virtual Private Networks. RFC 2764. Saatavissa: http://www.ietf.org/rfc/rfc2764.txt [viitattu 27.11.2009]

19. Metro Ethernet Forumin verkkosivut. Saatavissa: http://metroethernetforum.org/ [viitattu 25.11.2009]

20. Martini, L., Rosen, E., El-Aawar, N. & Heron, G. 2006. Encapsulation Methods for Transport of Ethernet over MPLS Networks. RFC 4448. Saatavissa: http://www.ietf.org/rfc/rfc4448.txt [viitattu 19.11.2009]

21. Lasserre, M. & Kompella, V. 2007. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. RFC 4762. Saatavissa: http://www.ietf.org/rfc/rfc4762.txt [viitattu 22.11.2009]